WNS
Extending Your Enterprise

Issue 2

Managing the Complexities of Governance, Risk & Compliance Requires

an 'Industry Focused' Business Process Management Partner

> "Analytics as well as deep industry and process knowledge create real value for companies by helping them achieve their GRC objectives"

-Views from Pervez Workingboxwalla, Corporate Senior Vice President, Risk Management & Audit, WNS Global Services

1. What are the key imperatives of a sound GRC program in the current business environment?

Pervez: You would have often heard that the world is flat. Well, the world might have become flat because of the outsourcing and offshoring phenomena, but the complexities of doing businesses have only escalated. The complexity graph is moving up steadily whereby businesses are exposed to new risks and threats, while at the same time governments are implementing legislations and imposing onerous compliance requirements on companies for the sake of protecting stakeholder interest and ensuring confidence and stability in the global economy. To that end, **'sophistication'** in Governance, Risk and Compliance (GRC) programs have assumed increased importance across all industries.

External and internal threats call for a 'robust' risk management organization: Businesses are at constant risk today from internal and external factors.

External threats: In my view, new business models and competitive pressures are the most crucial external factors threatening organizations today. Look at the retail industry. You don't need 50,000 square feet of store space to become a retailer today. You need a great website, warehousing facilities, an efficient logistics department and you are pretty much in business. Look at how video conferencing is impacting not just the airline business, but also the hospitality and car rental businesses. If business travel is curtailed, hotels as well as car rental companies will suffer too. These are examples of the immediate consequences of new business models on traditional

Featuring research from
Gartner

businesses. Businesses do get affected by many other indirect and collateral consequences. The bottom line however, is new business models are posing a real threat to traditional businesses.

Driven by competitive pressures, companies are being forced to take decisions to venture into areas that are way out of their risk appetite, because they want to stand out from their competitors. However, the irony is that, not taking such risky decisions may cause them to lose out to competition. When companies expand into new areas, be it a new geography or a line of business, they are met with a great deal of uncertainty and unforeseen risks. That's where robust risk management practices come into play.

Internal threats: Any industry at its very core is comprised of people, processes and technology. I believe that risks revolving around process and technology are easier to manage than people-related risks. For example, in services-based industries, people are core to the business and if companies want to de-risk themselves, there has to be a huge emphasis around people risk management. The liabilities that can arise from service failure, an error or worse, a breach caused by a single individual can pretty much sink the organization. That's where robust risk management practices come into play.

Increased focus on government regulations and compliance will require a 'specialist' taskforce: As companies focus on protecting market share by following the mantra of 'no risk, no gain,' governments are not sitting still. They are not allowing corporations to act recklessly, as there have been hard-hitting instances of aggressive business practices threatening to destroy confidence in capital markets. Governments are introducing legislations because, to a large extent, self-regulation has failed. For example, the Sarbanes-Oxley Act 2002 (SOX) was not implemented because Enron was the first company to fail in the history of corporate failures. Whenever there have been doubts about upholding shareholder interest or protecting economies from the aftermath of business malpractices, governments and / or regulators have been quick to introduce legislation. Most industries are dealing with a barrage of regulations and this will only accelerate with time. Governments will keep introducing legislation where they feel that investor interests could be compromised.

What is interesting is that, many of these legislations are principles-based. Organizations will need experts who can interpret those principles and design the business process and the reporting systems around it to be able to ensure compliance. This requires specialists who are both industry focused, understand the legislation and to a certain extent can even influence the drafting of the legislation.

Naturally, every company is now burdened with compliance obligations that it didn't have earlier. It is extremely important that companies are well geared in terms of having a proactive risk management team and an extremely knowledgeable compliance team to meet the challenges that the current business and legislative environment presents.

Governance structures have changed completely; 'transparency' and 'independence' are a must: In the past, responsibility for compliance rested only with the legal department. However, companies have to comply with not just local laws but even operational regulations. For instance, a person processing transactions must have working knowledge about the impact of his / her actions with respect to the regulations and / or legislation governing the business. Liabilities rest with the entire hierarchy, from the transaction processor right up to the Board level. As far as the Board is concerned, it must have an independent and transparent corporate governance tree that will make sure that the appropriate escalations are conveyed to the Board in a timely and accurate manner.

GRC programs are no longer a 'tick-in-the-box' option for organizations. GRC programs must be sophisticated enough to be able to deal with internal as well as external risks. Sophistication in the form of a robust risk management system, a specialist compliance task force and transparent and independent governance structures are the key to survive and more importantly thrive in the current business environment.

2. With sophistication / complexities defining GRC programs, are organizations equipped to deal with governance, risk and compliance on their own?

Pervez: Largely, the answer for a majority of organizations would be 'no' simply because of the complexities involved. For any organization, capital is a limited commodity. It is meant to be deployed to earn profits and maximize return on investment. Although businesses are focused on acquiring companies, assets, setting up business lines, expanding into new geographies and so on, investing in risk management has really not been a business imperative. Besides, with the internal threats and external complexities, the multiple business lines and diverse geographies that even medium size businesses operate in today, it is nearly impossible for such companies to have a GRC program that can deal with the multi-faceted challenges facing the organization.

At its root, GRC is a very specialized and complex field since it helps companies in identifying "what can go wrong". Most companies will eventually set up some form of GRC programs in place, but most of them will not have the resources to set up monitoring and reporting processes and systems.

3. Traditionally, enterprises have relied upon consulting firms to create GRC strategies. How do you think BPM companies can contribute to the organizational GRC goals of enterprises?

Pervez: You are right about the fact that in a large number of instances, organizations have employed consulting firms to design their GRC processes, systems and frameworks. Typically, a consulting firm owns the responsibility for making but not implementing the stated recommendations. While a consultant may advocate the adoption of best practices, real world circumstances require those best practices to be suitably tailored in order to achieve compliance goals on the one hand and business objectives on the other.

That's where organizations need an industry focused BPM partner that can work alongside it in implementing stated best practices as well as have enough industry knowledge and on-going organizational connect to be able to tailor such best practices to suit the organizational requirements.

BPM companies such as WNS, have deep industry knowledge and experience in managing business processes as well as outcomes for their clients. By outcomes, I mean not just the business impact but even the management of risk as well as ensuring compliance.

In my experience, while organizations have mature governance structures and robust risk management processes, it is the compliance program which usually lacks in investment. Organizations are forced to water down their compliance programs simply because they don't have the resources for it.

4. Can you please elaborate on the way a BPM partner like WNS would work with a client organization in order to achieve its GRC objectives?

Pervez: Yes absolutely. A BPM company such as WNS, which operates on an end-to-end vertical structure, understands the nuances of the industry as well as the specific business processes and the embedded legal and regulatory requirements that accompany it. Our knowledge of operating processes that we manage with an overlay of data analytics, gives us an edge to provide a much better, value added output. In fact we hold ourselves accountable to it by measuring our deliverables against specific service levels, which also include compliance against set requirements.

For instance, having worked on business processes for insurance firms from multiple geographies has built WNS's expertise in business processes for the insurance industry. Today we are in a competitive position to provide clients the support they need in complying with say, the Solvency II directive. Our services for Solvency II compliance would include actuarial modeling to facilitate reserving and pricing computations, critical for Solvency II capital estimation, as well as facilitating timely reporting and independent assurance on an ongoing basis. In addition, we provide country-specific regulatory reporting requirements and work across the entire value chain from data compilation, analysis and reporting. Besides, our data analytics-based fraud claim detection model has ensured significant savings on a continuous basis for one of our insurance clients.

Similarly, we work with leading banks to support them in areas such as compliance with OCC guidelines, thereby facilitating substantial cost saving apart from eliminating process redundancies through data analytics-driven solutions.

For all our clients, we have implemented a Business Process Risk Management and Audit (BPRMA) framework. The Business Process Risk Management (BPRM) framework includes the identification of process and system level risks for all outsourced processes, which is shared with our clients in the form of a 'risk register' in order for them to get a better view of risks in the offshore environment. Some of these risks, if not addressed, could even lead to non-compliance with regulations. These risks are then mitigated based on an agreed upon mitigation plan that is tracked in a periodically conducted joint governance meeting. The offshore risk registers are also available to our clients and can be consolidated with the onshore risk registers in order to arrive at the overall risk posture.

The Business Process Audit (BPA) framework requires a cyclical audit to be conducted on all outsourced business processes to ensure that the mitigation steps mentioned above are indeed implemented and address the stated risks. These audits also provide assurance around stated regulatory requirements, if any.

In the non-financial services sectors, clients have engaged with us to conduct operational risk reviews and SOX control testing on a continuous basis. With these solutions we have been able to highlight exceptions on a near real-time basis, thereby facilitating process improvements apart from ensuring regulatory compliance.

WNS's analytics offerings help clients understand the underlying risks associated with the business, while supporting their compliance initiatives. Integration of business processes to the overall GRC framework is critical for success.

Essentially, the key differentiators for a BPM company such as WNS are a **strong analytics backbone coupled with deep industry knowledge.**

5. What are the key tenets around GRC that an organization has to bear in mind while partnering with a BPM company?

Pervez: To begin with, outsourcing of business processes to a BPM company does not take away the responsibility around governance, risk and compliance from the organization.

However, as is evident from response to question number 4, organizations that partner with BPM companies that have deep industry knowledge as well as domain expertise are much closer to achieving their organizational GRC objectives.

Another important factor that comes to play here is analytics. Today, analytics plays an important role in risk management. Analytics helps identify risks of frauds and errors, likely to be missed by the human eye, at a mere glance of a transaction. Organizations must partner with BPM companies that can overlay analytics with the outsourced processes.

Analytical tools also facilitate risk measurement based on a combination of historical data, external data as well as scenario analysis. With the advent of Big Data and the availability of advanced analytics models, risk management can be strengthened, through real-time triggers on potential risks. This in turn, facilitates informed decision-making as well as timely risk mitigation.

Through analytical tools and techniques, the compliance function becomes more robust and facilitates deeper introspection of likely errors or frauds so that better controls can be implemented.

6. What should be the level of collaboration between the client's and the BPM Company's risk and compliance function?

Pervez: A quick response to this question would be 'absolute'. Given the complexity of the business as well as a plethora of regulations that most companies need to comply with, a lack of co-ordination and collaboration between the client and the BPM partner could have disastrous consequences.

The partnership approach that we follow at WNS is resonating very well with our clients. In my view, this kind of collaboration has worked well for achieving our clients' GRC objectives.

At WNS, we follow the 'Three Lines of Defense' model across all our client programs. Our First Line of Defense is the Quality function that manages the day-to-day compliance with stated program objectives. This even includes compliance checks around regulatory requirements that are specific to a client program.

The Second Line of Defense is the Risk Management and Audit function that manages the BPRMA framework and activities that I have mentioned earlier.

The client's as well as WNS's Second Line of Defense work very closely to interpret and weave in the internal policy as well as regulatory requirements into the processes we manage for the client. WNS's First Line of Defense then checks whether the objectives set by the risk management team are being met and reports the same accordingly.

The Third Line of Defense is always retained by the client's internal audit team, which holds full rights to audit WNS's operational risk management and compliance programs to ensure design efficiency and operational effectiveness.

Source: WNS

From the Gartner Files:

Predicts 2014: Advances in Risk Management Technology Will Improve Corporate Performance and Public Policy

Risk management influences the decisions of business and IT leaders, yet the effective use of IT solutions lags other management disciplines. CIOs and CISOs should look to future IT advances to enable better risk management programs and significantly improved corporate performance and public policy.

Key Findings

- IT organizations are improving the maturity of their security and IT risk programs, yet only 20% of companies report formally mapping key risk indicator (KRI) and key performance indicator (KPI) information.
- The traditional role of security remains in IT as a technical discipline, but the IT governance and risk management functions are increasingly moving out of IT to more closely align with business requirements and decision making.
- Over the past decade, IT has been democratized through mobile and social technologies that have shifted control of information to the user, and away from businesses, government agencies and other enterprises.
- CIOs and CISOs are hampered in their ability to provide a holistic view of risk data because of the often fragmented approach to collecting and analyzing risk data through the use of an array of governance, risk and compliance (GRC) tools or business intelligence (BI) solutions.

Recommendations

- Organizations should employ risk-adjusted value management, Gartner's methodology to integrate risk and corporate performance and improve the IT and security teams' knowledge of business processes, business outcomes and related IT dependencies.
- The CIO should work with the chief legal officer, chief marketing officer and chief strategy officer to align social media and analytics investment strategies to corporate strategic objectives that involve significant social implications.
- CIOs and CISOs should create a GRC Pace-Layered Application Strategy to address the application portfolio gaps, as well as anticipate the future needs of the business end-user community. This strategy must closely align with the needs of the enterprise risk management program to provide the holistic view of risk data that will be demanded by board members and senior executives.

Strategic Planning Assumptions

By 2016, 40% of large companies will integrate IT risk measurements with corporate performance, doubling from 20% in 2013.

By 2017, most new public policy will be established through direct social engagement of stakeholders, rather than through traditional regulatory means.

By 2016, a majority of CIOs and chief information security officers (CISOs) will adopt a GRC Pace-Layered Application Strategy to bolster the risk management program.

Analysis

What You Need to Know

The Strategic Planning Assumptions in this research highlight the risk management impacts on internal and external stakeholders, as well as the requirements for business and IT leaders to meet the future risk management challenges. The ever-changing and complex nature of risks facing companies in the future will dictate the need to change their approaches to conducting business and investing in technology solutions.

We have also highlighted two earlier predictions — one in which we missed, and one that is on track. We once believed that enterprises would make no distinction between corporate governance and IT governance, yet they remain divided activities. However, we are on track with our prediction that the majority of global financial services firms will still lack a holistic definition and understanding of enterprise risk management.

Strategic Planning Assumptions

Strategic Planning Assumption: By 2016, 40% of large companies will integrate IT risk measurements with corporate performance, doubling from 20% in 2013.

Analysis by: Paul E. Proctor

Key Findings:

- Gartner survey data in 2013 shows that only 20% of organizations report formally mapping KRI and KPI information that influences both IT and business unit decision making. However, 2013 was punctuated by serious distraction on cybersecurity concerns, materially increasing board and executive attention on IT risk issues. A gap remains between IT risk programs and executive understanding that can be bridged only by linking risk and security to corporate performance.
- IT organizations are improving the maturity of their security and IT risk programs. A major shift in security and IT risk program management has created a split between the traditional technology-driven parts of the security organization, and the governance, oversight and decision-making parts of the organization. The traditional role of security remains in IT as a technical discipline, but the IT governance and risk management functions are increasingly moving out of IT to more closely align with business requirements and decision making.
- The role of the new governance group is to balance the need to protect the organization with the need to run the business. This necessary alignment to business decision making is creating the opportunity to address the gap between

IT risk executives and non-IT executives. KRI and KPI mapping, done properly, integrates risk and corporate performance to influence both IT security and business decision making.

Market Implications:

As a result of these shifts, IT security departments are improving their knowledge of business processes, business outcomes and IT dependencies on the success of the organization. They are demanding new features and functions from traditional security products that enable them to map traditional security operational activities to business assets. For example, traditional vulnerability assessment tools are improving their asset classification capabilities to reflect business priorities.

Organizations are also increasing their spend on GRC capabilities to help them map risk-related elements to reporting and oversight for executives.

Recommendations:

- Organizations should explore risk-adjusted value management, Gartner's methodology to integrate risk and corporate performance.
- Organizations should improve the IT and security teams' knowledge of business processes, business outcomes and related IT dependencies.

Related Research:

- "Survey Analysis: Risk Management, 2013"
- "The Gartner Business Risk Model: A Framework for Integrating Risk and Performance"
- "The Gartner Business Value Model: A Framework for Measuring Business Performance"
- "Toolkit: Risk-Adjusted Value Management Workshop"
- "Enhance GRC With BPM for Improved Enterprise Risk Management"

Strategic Planning Assumption: By 2020, most new public policy will be established through direct social engagement of stakeholders, rather than through traditional regulatory means.

Analysis by: French Caldwell

Key Findings:

- Over the past decade, information technology has been democratized through mobile and social technologies that have shifted control of information consumption and much of the creation of information to the individual user, and away from businesses, government agencies and other enterprises. In addition to providing individuals with tremendous information access, these technologies enable individuals to connect and organize organically without the need for traditional organizational structures and hierarchies.
- There are a number of examples of direct social engagement where individuals or groups of individuals have bypassed traditional political and governing institutions to effect public policy change. The Arab Spring is the most oft cited example,[1] but change is occurring in developed democracies as well — for example:
  - In 2009, the Austrian science minister dropped funding for the CERN collider from the Austrian budget. An online petition spread by Twitter and Facebook gathered 32,000 signatures, and within two weeks, the government bent to public outcry and restored the funding.[2]
  - In late 2012, a Mississippi teenager pointed out that Gatorade contained bromine, which is also an ingredient in flame retardants. She made the startling assertion that people were drinking flame retardant, and started a petition on Change.org to have PepsiCo remove brominated vegetable oil from Gatorade. The petition reached over 200,000 signatures. In January 2013, PepsiCo's Gatorade organization, which maintains an online monitoring and response capability, announced that it was removing brominated vegetable oil from Gatorade.[3]
- Another phenomenon of emerging information technology is the dramatic increase in the volume of information that is being generated through the activities of individuals and their connections with one another, businesses and governments, and their use of personal devices and equipment. Big data analytics applied to this information can provide useful insights into behaviors and can influence outcomes. Examples include:
  - In response to the London riots in August 2011, the U.K. government briefly considered giving police new powers to block social media during riots. Within two weeks, that idea was shelved, and the government met with social media and mobile executives to determine how to coordinate better during an emergency.[4] Notably, the acting chief of London's police force called social media a useful intelligence asset. This point of view indicates that police may have used social analytics to pre-empt violence.
  - The 2012 U.S. presidential campaign was a watershed for combining social media and big data for direct social engagement. For example, the Obama campaign developed a social media initiative called Targeted Sharing, which enabled already persuaded voters to selectively contact a subset of friends on Facebook who were identified as more likely to commit. This was based on a predictive model that combined Facebook data with campaign information.[5]

Market Implications:

- Seemingly small issues can be amplified through social media. As the use of social technologies proliferates, risk events that may well have stayed below the public radar will be amplified by nonfinancial stakeholders. Social technologies will cause even more risks to be amplified beyond corporate risk tolerances.
- The Arab Spring, Austrian CERN funding and Gatorade examples illustrate that public policy and even significant political change can be made without regard, and even in direct opposition, to traditional political and governmental institutions. The asymmetry of traditional institutions' processes, compared with a technology-savvy knowledge polity, highlights the organizational power of social and mobile technologies.
- On the other hand, the Gatorade, London riots and U.S. presidential campaign examples illustrate how traditional institutions can apply social analytics to respond to and even influence outcomes.

Near-Term Flag: By 2017, several large national regulators will have established social-media-listening capabilities to assess public sentiments on policy issues.

Recommendations:

- CIOs and other IT leaders should set the tone that social issues matter and build relationships with legal, PR, marketing and other organizations that are tracking the issues. The CIO should work with the chief legal officer, chief marketing officer (CMO) and chief strategy officer to align social media and analytics investment strategies to corporate strategic objectives that involve significant social issues.
- CMOs should apply social media listening to public policy issues that affect the company, such as trade, privacy, taxes, executive compensation, crisis and disaster response, and sustainability, and should be especially cognizant of those issues when planning social media campaigns for new products and services. Social media campaigns can amplify pre-existing issues significantly. Timing is everything — social media is an interactive forum — so these campaigns should be carefully thought through before being launched.

Related Research:

- "Maverick* Research: Black-Hat Data Science Will Impact Society and Your Business"
- "Three Best Practices for Implementing Social Media Compliance"
- "Gartner Fellows Interview With Patricia Flynn, Vice President at Fidelity Investments: Managing Social Media Compliance"
- "Security Tools for Control of Social Media Usage"
- "Answer Seven Critical Questions Before You Write Your Social Media Policy"
- "Social Media Governance: An Ounce of Prevention"

Strategic Planning Assumption: By 2016, a majority of CIOs and CISOs will adopt a GRC Pace-Layered Application Strategy to support the risk management program.

Analysis by: John A. Wheeler

Key Findings:

- According to a recent Forbes Insights and Deloitte survey, 91% of companies are working to reorganize and reprioritize their risk management programs by 2015.6 This effort is driven by the increasing risks associated with a more global, interconnected business environment that requires a more holistic view of risk data across the enterprise.
- However, CIOs and CISOs are hampered in their ability to support such a holistic view because of the often-fragmented approach to collecting and analyzing risk data through the use of an array of GRC tools or BI solutions. Some companies have turned to investments in enterprise GRC (EGRC) software platforms to integrate and aggregate their risk data. While this is a good first step in setting the foundation of an effective GRC application strategy, it typically provides only a data repository to serve as an enterprise's GRC "system of record."
- What is really needed to provide a holistic view of risk data is a well-designed GRC application portfolio that reaches all the business constituencies (that is, internal business managers, as well as external parties, third-party vendors and partners) through the variety of risk-related contexts (that is, financial, operational, reputational, life or safety, legal, and IT). With an ever-changing set of GRC-related use cases, enterprises can best articulate and manage the application portfolio through Gartner's Pace-Layered Application Strategy (see Note 1).

Market Implications:

- By refocusing investments in GRC technology using a pace-layered approach, CIOs and CISOs can more easily meet the risk management demands from business managers. As a result, they can increase the usage of GRC applications, as well as improve the quality and integrity of risk data. Feedback from our clients indicates that a GRC application strategy that includes a wider array of application use cases is required. Moreover, in a 2013 Gartner survey conducted for "Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms," 152 EGRC platform users demonstrated the variety of use cases desired by end users (see Figure 1).

The wide variety of use cases will require different levels of care and feeding for related GRC applications, and could drive the need for purpose-built GRC applications that integrate with EGRC platforms that serve as the primary system of record.

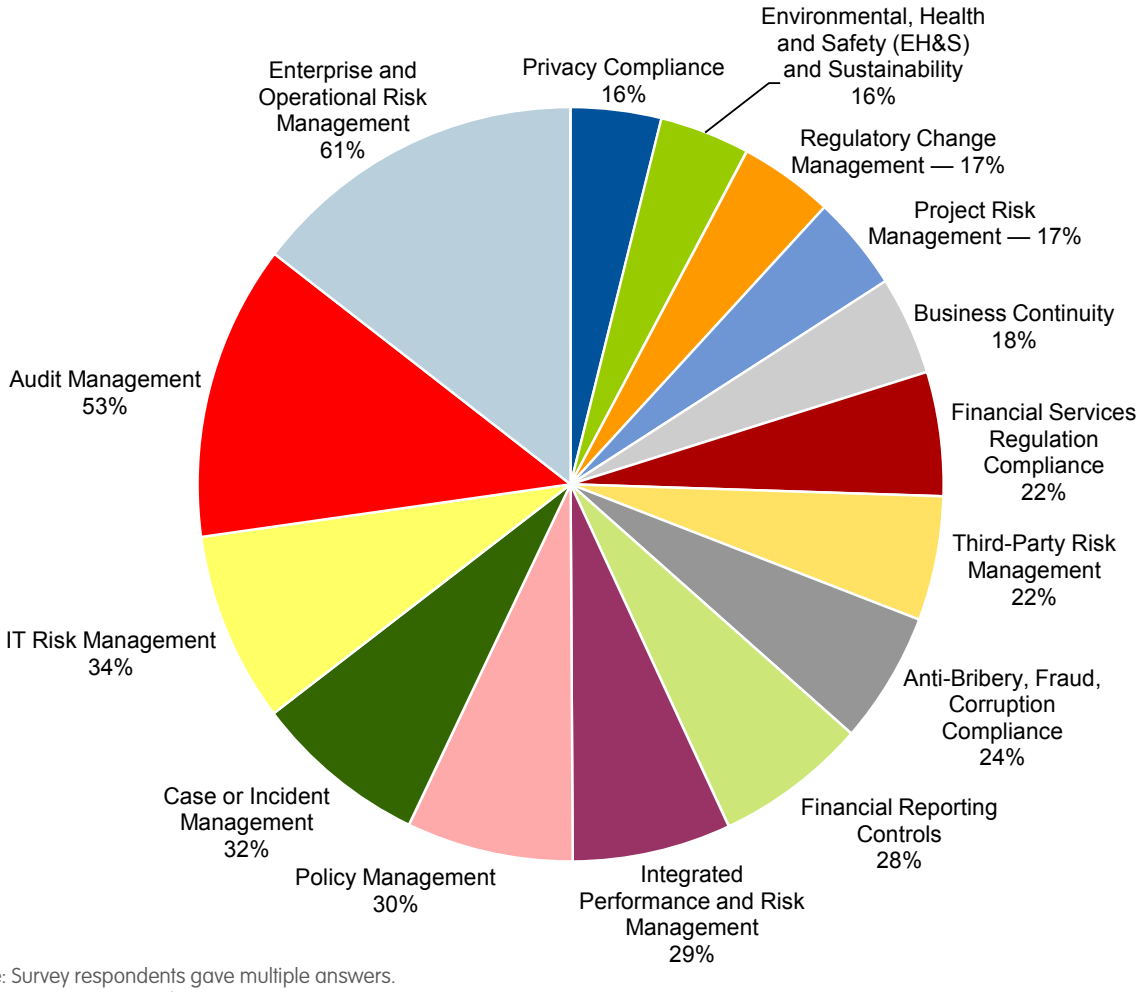
Recommendations:

- CIOs and CISOs should assess the composition of their current GRC application portfolios against the use cases that are required by business end users. The gaps in the GRC application portfolio should be highlighted for further analysis and potential investment.
- In addition, CIOs and CISOs should create a GRC Pace-Layered Application Strategy to address the application portfolio gaps, as well as anticipate the future needs of the business end-user community. This strategy must closely align with the needs of the enterprise risk management program to provide the holistic view of risk data that will be demanded by board members and senior executives.
- GRC software vendors should simplify integration with advanced analytics tools, and build out a portfolio of targeted solutions from both the vendor and third parties.

Related Research:

- "Use the Pace-Layered Application Strategy to Understand Your Applications Portfolio"
- "How to Use Pace Layering to Develop a Modern Application Strategy"
- "Use a Pace-Layered Application Strategy to Improve IT's Relevance to the Business"
- "Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms"

FIGURE 1
Top Use Cases for Enterprise GRC, 2013



Note: Survey respondents gave multiple answers.
Source: Gartner (November 2013)

A Look Back

In response to your requests, we are taking a look back at some key predictions from previous years. We have intentionally selected predictions from opposite ends of the scale — one where we were wholly or largely on target, as well as one we missed.

On Target: 2009 Prediction — Through 2013, the majority of global financial services firms will still lack a holistic definition and understanding of enterprise risk management (see "Predicts 2010: Operational Technologies Present Threats and Opportunities in Banking and Investment Services").

While we are a full five years removed from the global financial crisis of 2008, this prediction remains true. A significant piece of evidence that this prediction is on target is the issuance of guidance by the Basel Committee earlier this year.7 In association with the Basel III capital accord, this new guidance provides a set of risk data aggregation and risk reporting objectives that globally significant financial institutions must achieve by 2016. It recognizes the inadequacy of IT and data aggregation capabilities that was evident during the financial crisis and continues today. So, while some financial institutions may have a holistic definition of enterprise risk management, their understanding of enterprise risk management will be severely limited by their inability to aggregate and report risk data.

Missed: 2010 Prediction — By 2014, enterprises will make no distinction between IT governance and corporate governance (see "Predicts 2011: In the 'New Normal,' Governance, Risk Management and Compliance Are Inseparable From Business Realities").

IT is a central component of most, if not all, businesses today, yet most organizations still primarily view governance of IT as a separate exercise. Updated frameworks like the recently released COBIT 5, or the COSO Internal Control — Integrated Framework and ISO 22301:2012, make an attempt at strengthening the link between corporate and IT governance. However, Gartner's 2013 Global Risk Management Survey shows that the two activities are still disconnected. Only 46% of survey respondents indicated that the board members utilize IT risk management data to influence their decision making. Without the regular reporting and usage of IT risk management data at the board level, IT and corporate governance activities will remain disappointingly divided.

Gartner Recommended Reading

- "Survey Analysis: Risk Management, 2013"
- "Toolkit: Risk-Adjusted Value Management Workshop"
- "Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms"
- "Enhance GRC With BPM for Improved Enterprise Risk Management"
- "Use the Pace-Layered Application Strategy to Understand Your Applications Portfolio"

Evidence

[1] G. Wolfsfeld, E. Segev and T. Sheafer, "Social Media and the Arab Spring: Politics Comes First," The International Journal of Press/Politics, 16 January 2013.

[2] M. Banks, "Austria Performs U-Turn Over CERN Pull-Out," Physics World, 19 May 2009.

[3] M. Eng, " PepsiCo to Take Controversial Ingredient Out of Gatorade," Chicago Tribune, 25 January 2013.

[4] The Associated Press, "U.K. Opts Not to Block Social Media During Riots," CBC News, 25 August 2011.

[5] K. Carter, "Q+A With Rayid Ghani, (Former) Chief Scientist, Obama for America," ADMA, 19 June 2013.

[6] Forbes Insights and Deloitte, "Aftershock: Adjusting to the New World of Risk Management," June 2012.

[7] "Principles for Effective Risk Data Aggregation and Risk Reporting," Basel Committee on Banking Supervision and Bank for International Settlements, January 2013.

Note 1
Gartner's Pace-Layered Application Strategy

Gartner's Pace-Layered Application Strategy is a methodology for categorizing, selecting, managing and governing applications to support business change, differentiation and innovation. Gartner defines the three application pace layers as:

- **Systems of record** — Established packaged applications or homegrown legacy systems that support core transaction processing and manage the organization's critical master data. The rate of change is low, because the processes are well-established and common to most organizations, and often are subject to regulatory requirements.

- **Systems of differentiation** — Applications that enable unique company processes or industry-specific capabilities. They have a medium life cycle (one to three years), but need to be reconfigured frequently to accommodate changing business practices or customer requirements.

- **Systems of innovation** — New applications that are built on an ad hoc basis to address new business requirements or opportunities. These are typically short-life-cycle projects (zero to 12 months), using departmental or outside resources and consumer-grade technologies.

Source: Gartner Research, G00259088, John Wheeler, French Caldwell, Paul Proctor, 7 November 2013

About WNS

WNS (Holdings) Limited (NYSE: WNS) is a leading global business process solutions company. WNS offers business value to 200+ global clients by combining operational excellence with deep domain expertise in key industry verticals, including Travel, Insurance, Banking and Financial Services, Manufacturing, Retail and Consumer Packaged Goods, Shipping and Logistics, Healthcare and Utilities. WNS delivers an entire spectrum of business process outsourcing services such as finance and accounting, customer care, technology solutions, research and analytics and industry-specific back-office and front-office processes. WNS has delivery centers world-wide, including China, Costa Rica, India, the Philippines, Poland, Romania, South Africa, Sri Lanka, UK and US.

WNS
Extending Your Enterprise