books24x7®

ExecBlueprints™

in partnership with Aspatore Books

Action Points

I. **What Is "GRC"?**
The term GRC, which stands for governance, risk management, and compliance, is a revolutionary idea in that it describes an integrated approach to managing the flow of information, processes, and technologies across an organization so that management can systematically achieve objectives while addressing uncertainty and acting with integrity.

II. **The Bottom Line**
To develop a GRC model, your company will need to invest resources – and you may not see returns right away. However, since a comprehensive execution also entails monitoring, you should soon have data that will answer the following questions: Are you experiencing fewer incidents and fines? Lower audit costs? Increased revenues stemming from improved decision making?

III. **Must-Have Benefits of a GRC Model (and Pitfalls of a Siloed Approach)**
In today's risk-prone business environment, responding to threats and complying with regulations can no longer be considered one-off activities, but must be incorporated into an integrated process that ensures that managers have the information they need to make decisions that will leverage opportunities while protecting the organization.

IV. **The Golden Rules for Developing a Sound GRC Framework**
A unified approach to governance, risk management, and compliance is a capability, not a department or program, and migrating to this approach usually requires a culture change to motivate leaders to link their "risk philosophy" to strategy development, collaborate with others, and empower employees to think like risk managers.

V. **Essential Take-Aways**
A well-designed GRC model will more effectively manage your company's risk and compliance profile than siloed approaches. Key components include leadership engagement, enterprise-wide oversight, central document repositories, department-level risk management, and a secure IT infrastructure that keeps the information flowing.

Contents

Compliance leaders from OCEG, Pacific Gas and Electric Company, MetricStream, and Acolyst on:

Governance, Risk Management, and Compliance: Creating the Right GRC Strategy for Your Company

Carole S. Switzer
Co-Founder and President, OCEG

Anil Suri, Ph.D.
Vice President and Chief Risk and Audit Officer
Pacific Gas and Electric Company

Gaurav Kapoor
Chief Operating Officer, MetricStream

Valeh Nazemoff
Senior Vice President, Acolyst

In the world of business (and innovation), "risk management" does not necessarily mean risk prevention. Often, there will be core areas where your company is willing to take risks in order to generate returns, such as entering a new market or developing a new product. Rather than avoid all risk, leaders of successful organizations assess the risks inherent in any situation and use them to drive company vision, strategies, plans, and processes. This ExecBlueprint describes an integrated approach for managing performance, risk, and compliance through centralized governance processes. It is called "GRC" (governance, risk management, and compliance), and it provides a framework for sharing policies, processes, and documents at the enterprise level to improve communication, create organizational efficiencies, and reduce unnecessary risk. How can GRC benefit an organization? When leaders are able to define their "risk appetite" and quantify all the risks facing them, they can make more appropriate strategic decisions, thereby giving their organizations a competitive advantage. ■

About the Authors

Carole S. Switzer

Co-Founder and President, OCEG

Carole Switzer is the co-founder and president of the Open Compliance & Ethics Group (www.oceg.org), a global nonprofit think tank, and online community of more than 40,000 individuals in more than 70 countries, that provides standards, guidelines, and online resources to help organizations achieve principled performance.

Ms. Switzer is a recognized leader in the concept of integrated governance, risk management, and compliance (GRC) and is a principal author of the open source *OCEG Red Book GRC Capability Model*. She is frequently published in leading business magazines and lectures on GRC throughout the world. She advises university professors in several countries on how to teach GRC concepts in graduate programs and developed OCEG's on-demand training course series, GRC Fundamentals. In 2010, she was honored with a lifetime membership in the Institute for Risk Management and most recently was recognized in the 2012 edition of the *Martindale-Hubbell Bar Register of Preeminent Women Lawyers*.

☛ *Read Carole's insights on Page 3*

Anil Suri, Ph.D.

Vice President and Chief Risk and Audit Officer, Pacific Gas and Electric Company

Anil K. Suri, Ph.D., is responsible for overseeing the company's enterprise-wide risk management, internal audit, compliance and ethics, market and credit risk management, insurance, and corporate security functions. He joined PG&E in 2010 after owning and operating a risk management consultancy in New York, where he advised utility-industry senior management in the renewables, fuel supply and new generation markets, and managed market and credit risk of generation assets, pipelines, and regulatory assets for utilities and other energy providers.

Prior to that, Dr. Suri founded the electricity hedging business as managing director of Wells Fargo Bank N.A. He served as CEO of E-lecTrade Inc., which provided electricity procurement, sales, structuring, and trading services for the energy industry, and was a founding partner of The Risk Partners LLC, where he marketed risk advisory and risk transfer services to utilities, pension funds, and insurance companies.

Dr. Suri has also worked as a scientist at Yale University and as an oceanographer at Harvard University, where he earned his Ph.D. in fluid turbulence.

☛ *Read Anil's insights on Page 7*

Gaurav Kapoor

Chief Operating Officer, MetricStream

As the chief operating officer of MetricStream, Gaurav Kapoor has the overall responsibility for sales, marketing, customer advocacy, the partner ecosystem, and ComplianceOnline.com. Until 2010, he also served as the company's CFO. During this time, he led MetricStream's financial strategy as well as sales, marketing, and partnerships. He also launched ComplianceOnline.com, a MetricStream business unit which has grown to become a leading online GRC community and content property.

Mr. Kapoor came to MetricStream from OpenGrowth, an incubation and venture firm where he helped build and grow several companies including ArcadiaOne and Regalix. Prior to that, he spent several years in marketing, operations, and business roles at Citi in Asia and the U.S.

He also serves on the board of Regalix, a digital innovation and marketing company.

☛ *Read Gaurav's insights on Page 11*

Valeh Nazemoff

Senior Vice President, Acolyst

Valeh Nazemoff, forthcoming author, serves as senior vice president of Acolyst where she specializes in helping executives and decision makers map, design, and achieve strategic initiatives such as cloud computing, mobility, big data, and business process improvement through business performance management.

Ms. Nazemoff has led project teams in formulating strategic visions, tactical roadmaps, and assessments of large, complex enterprise-wide clients. Projects include collaboration with organization's IT, legal, financial, and other departments. She has guided clients on ways to improve organizational communication and behavior by formalizing an integrated GRC and Legal program, understanding the importance of properly documented internal Service Level Agreements (SLAs), taking proactive actions with change management and incidents, establishing a universal common language with metadata using data modeling, visualizing where the data resides, and much more.

Ms. Nazemoff has also judged and evaluated emerging technologies for VARBusiness Technologies of the Year Award. Additionally, she served on the editorial cabinet committee from 2004-2007 for *CRN* magazine, where she had the opportunity to rate the performance of various IT/non-IT executives.

Recognized on *CRN*'s 2013 Women of the Channel, she frequently contributes to UBM Tech and CA Technologies' SMART Enterprise Exchange publications. She recently presented a workshop at the GRC Summit in Boston, MA.

☛ *Read Valeh's insights on Page 18*

Carole S. Switzer

Co-Founder and President, OCEG

Defining GRC

A couple of years ago, you could attend any large conference on GRC and likely hear as many definitions of GRC as there were sessions at the event. Today, that is changing, as a unified view and definition of GRC has emerged. First and foremost, most people now recognize that a unified or integrated approach to governance, risk management, and compliance (GRC) is a capability, not a department or program. An organization with a strong GRC capability has more risk awareness and thus better strategic planning, and is more likely to perform in accordance with its established goals.

The universal GRC goal is what we at OCEG refer to as "principled performance"; the ability to reliably achieve objectives while addressing uncertainty and acting with integrity. GRC is the capability — comprising people, resources, processes, and technology — that enables principled performance. GRC represents taking an integrated approach to the governance, management, and assurance of performance, risk, and compliance; however, this is not easy to turn into a useful acronym, so the shorthand use of GRC has taken hold.

Integrating GRC

Integrating GRC does not mean creating a mega-department of GRC and doing away with decentralized or programmatic approaches to risk and compliance management. Rather, it is about establishing a holistic approach that ensures the right people get the appropriate (and correct) information at the right times. Having unified vocabulary and taxonomies for information; establishing common repositories for data, documents, and information; creating standardized procedures and templates for things such as policies and training; ensuring regular and consistent communication between and among all relevant roles including strategic decision-makers — these are all aspects of an effective GRC capability.

OCEG issues free, open-source process standards for establishing an integrated GRC approach in our GRC capability model (commonly referred to as "the Red Book"), now available in version 2.1. Since we began drafting the first version in 2003, the Red Book has had contributions from hundreds of experts in governance, risk, compliance, legal, audit, information technology, operations, and other relevant roles in business, academia, government, industry, advisory, and solution provider organizations. It has also been through two rounds of public exposure review with thousands of reviewing individuals from many countries. Naturally, I recommend it as the primary source of guidance for developing an integrated GRC capability, along with other OCEG resources such as the companion GRC audit guide and toolkit ("the Burgundy Book"),

The universal GRC goal is what we at OCEG refer to as "principled performance": the ability to reliably achieve objectives while addressing uncertainty and acting with integrity.

Carole S. Switzer
Co-Founder and President
OCEG

Carole S. Switzer
Co-Founder and President
OCEG

"When an organization, and everyone making decisions within it, are appropriately *confident (because you can also be confident when you should not be) and understand the organization's risk appetite and strategic goals, they can take advantage of risk in a way that others cannot, without going beyond established risk thresholds and tolerances. That is a real competitive advantage."*

- *Organization's co-founder and president*
- *Recognized leader in the concept of GRC*
- *Principal author,* OCEG Red Book GRC Capability Model
- *Recognized in 2012* Martindale-Hubbell Bar Register of Preeminent Women Lawyers

Ms. Switzer can be e-mailed at carole.switzer@execblueprints.com

GRC Technology Solutions Guide, standard GRC-related definitions at the online glossary established by OCEG (www.grcglossary.org), and various OCEG whitepapers, illustrations, and handbooks.

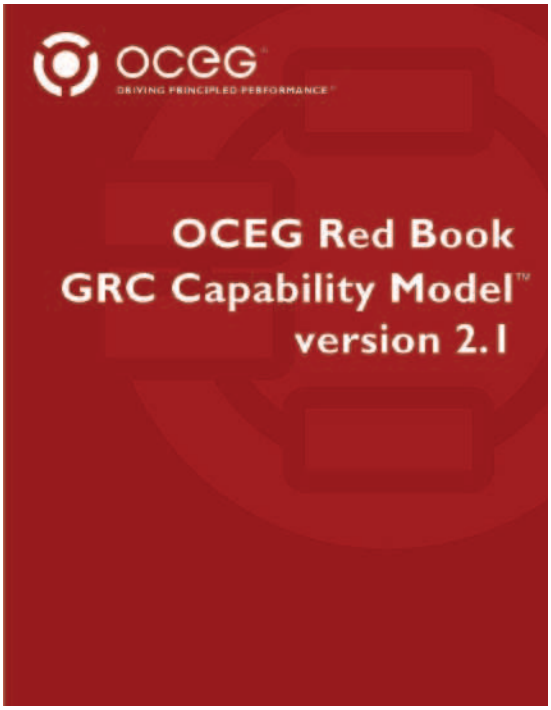
Many of the organizational steps recommended in the Red Book have been implemented by the companies that are engaged in improving GRC capability, as seen in the responses to our GRC maturity survey. In particular, these companies are more likely to have established enterprise-wide independent roles for a chief compliance officer and a chief risk officer, as well as compliance and risk committees to ensure communication and coordination of activities. Many have also established enterprise-wide committees for addressing their GRC capability needs, and these include participants throughout the organization in risk, compliance, audit, finance, information technology, legal, human resources or training, and strategic roles.

Expert Advice

As co-founder and president of OCEG, the nonprofit think tank that develops GRC standards, guidance, and vocabulary, I have spent a great amount of time working with others to refine the definition of GRC so that it has meaning for chief executive officers and other senior business leaders in the context of their strategic and performance goals. While GRC *denotes* governance, risk management, and compliance, it *connotes* much more than those three terms.

It is important to remember that organizations have been doing governance, risk management, and compliance management for a long time – in that sense GRC is nothing new. But despite this history, many are still not engaging in these activities in a mature way, nor have these efforts supported each other to enhance the likelihood of achieving corporate objectives, and in that sense GRC, as we understand it today, is totally revolutionary.

OCEG Red Book
GRC Capability Model Version 2.1

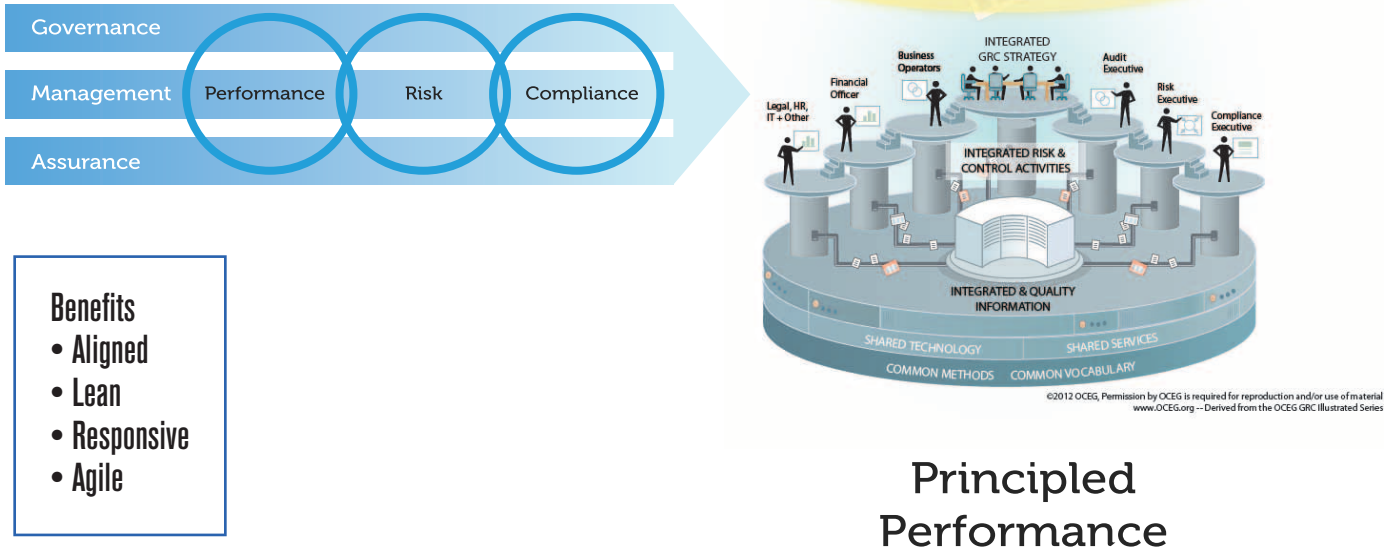


A free version of the Red Book (as pictured), the GRC Maturity Survey report, and other core OCEG materials are available to the public by registering for free at www.oceg.org.

Benefits of an Integrated Approach to GRC

The benefits of integrated GRC and the negative impacts of a siloed approach are two sides of the same coin. In our recent GRC maturity survey, we had over 500 participants, with more than two-thirds providing information on the positive outcomes they have gained from being on the "GRC journey," and the remainder providing a clear picture of the failure of a siloed structure. In particular, the difference between these two groups was striking in the levels of confidence they have, or do not have, in what they know about threats to the organization and their ability to effectively manage those threats. Those who are engaging in GRC, as compared to those who remain siloed, are often twice or even three times as likely to feel confident that they can identify risks and

Positioned for Competitive Advantage



Benefits
- Aligned
- Lean
- Responsive
- Agile

Principled Performance

compliance requirements; that they have selected and are implementing the right controls; and that they can evaluate their performance against established objectives.

What does this mean? I think that having this confidence enhances the critical attributes that a company needs to be competitive. This includes being aware of what is going on both internally and externally, so that you can evaluate information before taking action and respond appropriately. It means being agile, moving not just quickly but with the ability to shift direction when called for to avoid threats or grasp opportunities. It allows for the organization to be both lean, with more muscle and less fat, if you will, and more resilient so that it can recover from adversity.

Risks of a Heavily Siloed Approach

In general, we find from our research that the more siloed the risk and compliance operations, the less likely it is that critical information about these areas of concern is shared with strategic decision makers in a timely fashion; and, as you might expect, the less likely it is for risk and compliance roles to be included in strategic decision-making meetings since they are simply viewed as people who want to "put the brakes on" business decisions. The greatest risk of a heavily siloed approach is that wrong decisions are made, which cause the organization to face too much risk or fail to grasp opportunities.

But there are other risks identified in our research as well. Siloed operations spend too many resources trying to reconcile disparate information, have gaps and unnecessary overlaps in activities, put too much burden on the business by failing to coordinate schedules and requests for information, and even worse, may create new risks themselves.

Overall, it is clear that more companies are now recognizing the true value of maturing their approach to GRC, and not just for the benefit of reducing compliance

costs or being more able to avoid major compliance catastrophes. While these are great goals, the organizations that are succeeding today are those with leaders who appreciate how a consistent, integrated GRC strategy is really about running their business better and enabling them to make strategic decisions with a competitive advantage. ■

Anil Suri, Ph.D.

Vice President and Chief Risk and Audit Officer, Pacific Gas and Electric Company

Defining GRC

I think about governance, risk management, and compliance (GRC) in the following way: 1) we have to comply to stay in business; 2) we have to ensure we are managing risk appropriately; and 3) we have to make sure that we have the right governance in place to provide assurance that we are, in fact, doing all of the things we say we are doing and that they are effective.

There are several steps required to achieve integration across the three strategic areas of GRC. The organizational structure should be defined in such a way that it makes risk and compliance everybody's business. Everyone in the company needs to comply with certain requirements, and all employees have to manage risk. Next, you have to train people to think in "risk" terms: systematically look at your operations and the services you provide, and use risk to inform your priorities and plan your work. We believe that everyone in PG&E has a part to play in managing risk to the company. Our goal is that everyone in the company should act and think like a risk manager. Using a common risk glossary and consistently applying the definitions helps the organization speak in the same language. Lastly, after you have completed your process design and have your organizational structure in place, you need to have an effective information management system to support the flow of information up and down the chain.

If you are doing GRC effectively, you should be reducing the volatility that your investors see in your business; you should have fewer safety incidents, fewer liabilities, better operational performance, and so forth.

Anil Suri, Ph.D.
Vice President and Chief Risk and Audit Officer
Pacific Gas and Electric Company

When we talk about GRC, the risk piece is the most important aspect for our organization, because that is what we do — we manage safety risk, risks to reliability, and risks that threaten affordability of service for our customers. Risk is what drives our company's vision, strategies, plans, and processes. Our company is in a leading position for risk management in the utility industry. We've implemented a new governance structure for managing risk, augmented our risk management expertise, and embedded risk management within the lines of business at our company. In addition, risk management underpins our company's integrated planning process whereby risks and associated mitigations are explicitly discussed in strategy and budgeting discussions. This is considered best-in-class among our peers.

Developing a GRC Strategy

When we created our GRC strategy, we developed our risk standards based on ISO 31000, which we adapted and modified for our company. Using these standards as our foundation, we developed procedures for each of our lines of business that enable them to identify and evaluate risks, develop and implement risk response plans, and implement controls and metrics to ensure that we are following through with commitments and monitoring the risk profile. Metrics and monitoring are critical to providing the data needed to demonstrate progress.

Anil Suri, Ph.D.
Vice President and
Chief Risk and Audit Officer
Pacific Gas and Electric Company

"The GRC process is so much more than an add-on requirement; it is a change in how you manage the business."

- *Responsibilities include PG&E's enterprise-wide risk management, internal audit, and compliance and ethics functions*
- *Previously managing director, Wells Fargo Bank, N.A.*
- *B.S., Mechanical Engineering, Indian Institute of Technology, New Delhi*
- *M.B.A., Finance, Columbia Business School*
- *Ph.D., Fluid Turbulence, Harvard University*

Mr. Suri can be e-mailed at anil.suri@execblueprints.com

Overall, it is a very cyclical process, because it is important to continue to identify new risks as they arise or as the profile changes.

We set up our organizational structure so that each line of business has its own risk and compliance committee. The senior vice president of each unit serves as the chair of each committee, so the accountability is straightforward. These individuals are responsible for managing risk throughout the organization. They have all appointed risk managers as well. These individuals make sure the work gets done, shepherd the committee, and bring the operational expertise specific to that line of business. Having a partner within the line of business who knows operations and who is helping to evangelize risk management is critical to moving the process forward. Issues and policies that need cross-organization attention also receive oversight through a companywide risk policy committee.

In addition, risk is foundational to our strategic planning process. Each year our senior executives attend a day-long discussion on the company's key risks, called Session D: the Risk and Compliance Session. The purpose of the annual Session D is to set the foundation to link risk management to strategy development and resource prioritization. This annual process instills alignment between the company's strategic objectives and rigorous risk management.

Working with Vendors, Consultants, and Technology

While we love off-the-shelf products and approaches, GRC as a discipline is not at a stage where these products can be easily applied across the board. As a result, I think vendors and consultants need to be true partners to organizations and help them think strategically about how to have effective governance and compliance. Vendors and consultants need to be prepared to work in possibly unfamiliar frameworks. For example, we have some partners who are coming from the financial industry, and not all of those practices are applicable to our business. As a result, we need our partners to provide off-the-shelf products that are flexible while providing enough of a tool set so we don't have to design everything from scratch.

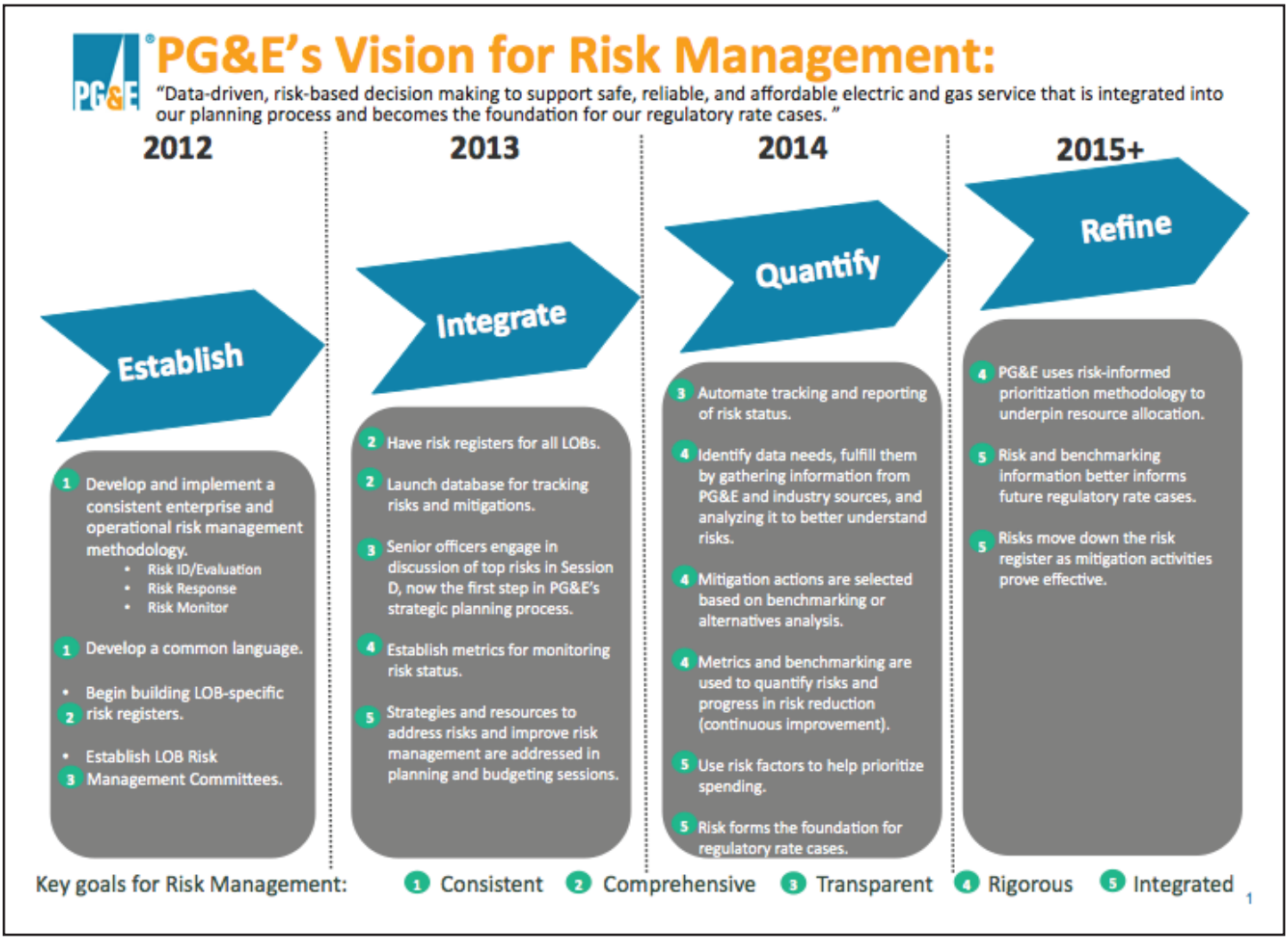
Our use of technology in GRC is an evolving process; we would like to leverage these tools to play a bigger role in collecting and analyzing data. Today it is premature for us to deploy a complete technology solution without first having the right process and structure in place. At the moment, we have a fairly basic information management system where we are tracking and archiving documentation for all of our risks and action items. As our GRC processes mature, we would like to see it move to a system that is integrated with our other business technologies so that real business intelligence can be generated.

Creating an Effective GRC Roadmap

There are three elements to an effective roadmap. First, you need unqualified and enthusiastic support from senior leadership. Our board members, along with our CEO and president, are all very much behind our push to become risk-based. Without that support, you will never be able to overcome the obstacles you need to be effective. The second part is having the right organizational structure as previously described, so that it creates accountability and depth of involvement. When you have risk and compliance committees at the business level, you can create accountability at each step of the business. Those leaders are then holding their direct reports accountable, and it cascades throughout the entire organization. It is our goal to have the entire organization wholeheartedly believe and work in a risk management mindset. My team of risk professionals attends all of the committee meetings and provides support to the line of businesses

Expert Advice

Influential Trends The biggest trends in operational risk affecting us are our aging infrastructure and the move toward stable affordability. Our infrastructure profile is undergoing a process of change – it is getting older, it needs work, and it needs replacement, which puts price pressure on our customers. Customers end up paying for these improvements, so we need to be able to use risk factors to prioritize our work on their behalf and ensure we are addressing the highest risks first. Use of a rigorous alternatives analysis to document benefits to safety, reliability, and affordability of mitigation options provides transparency and results in better decision making. Once you can use risk to prioritize, then it becomes possible to balance affordability with safety and reliability.



to maintain momentum and consistency of our risk standard. Ultimately, the third piece is having a good information management system that allows for transparency and accountability of the risk response plans.

Measuring and Evaluating GRC Strategies

Once you have a way to allocate resources based on risk, you can compare to the alternative, when you didn't have those mechanisms in place, or when you were acting on an instinct. As a whole, measuring GRC activities is difficult; once you have an analysis in front of you, you will probably say, "Well, I would have done it that way, anyway." Return on investment can be measured either as improvement in your efficiency of resource allocation based on risk or as reduction in the volatility of results from operations of the company. However, the volatility measurement does require a few years of consistent application and data. If you are doing GRC effectively, you should be reducing the volatility that your investors see in your business; you should have fewer safety incidents, fewer liabilities, better operational performance, and so forth. That translates into truly stable higher returns, which will eventually be the ultimate demonstration of ROI.

There are also ways to benchmark the efficacy of GRC, such as monitoring the progress of the risk standard and procedures. You can benchmark the components of the efforts, such as your efficacy with mitigation activities. For example, we manage a big network of power distribution, and we can compare our results in this area to others. This is only possible because we are able to provide transparency through our GRC system.

Identifying Key Challenges in GRC Strategies

The biggest obstacle we have encountered in the GRC process has to do with culture and changing the way of thinking and decision making. You just have to find a way to encourage leaders to actively think in terms of risk management — relying more on real data to make risk-informed decisions — and understand how this approach will help them manage their business better to achieve their strategic objectives. Most of our leaders have been thinking about risk all along, so we just need to be more data-based and transparent about it. The real challenge is to successfully achieve that transformation of thought.

Future Directions for GRC Planning

We have implemented quite a few changes over the last year and a half, so for us, it is about continuing on the path of implementation, and I don't expect that we will make any major changes to our GRC approach. The main evolutionary step we hope to take by next year is better quantification. We want to be as data-driven as possible when it comes to risk management. The chart above shows the long-term vision for PG&E's risk management. ■

Gaurav Kapoor

Chief Operating Officer, MetricStream

Enterprise-wide Responsibility for GRC Oversight

The challenge of demonstrating greater accountability and transparency, and creating an ethical, compliant, risk-aware, and well-governed organization doesn't just rest with senior management anymore. The notion of "enterprise GRC" means that every employee across the enterprise plays an active role in contributing to the development of a new kind of corporate culture that reflects the values of the firm, while asserting that business is being done in a risk-aware, legal, ethical, and compliant manner.

Employees today are empowered to play a more active role by leveraging real-time risk intelligence that can be used to create actionable insights that support decision makers. The C-suite relies on senior management to provide a comprehensive and holistic view of their organization's risk and compliance position. Further, board members are demonstrating greater oversight and demand an intimate purview into the company's governance, risk, and compliance programs and processes. This "no mistakes" business climate has put significant pressure on the business, spawning an urgent need to develop new robust and integrated governance, risk, and compliance (GRC) initiatives across the organization. In order to do this well, organizations need to break down the silos, reduce duplicative efforts, and identify opportunities for greater efficiencies. Thus, many organizations are turning to technology to help automate and manage the entire gamut of their GRC initiatives.

Organizations must focus on building and implementing an integrated GRC solution that enables the enterprise to manage the entirety of its GRC initiatives on a single and central platform.

Gaurav Kapoor
Chief Operating Officer
MetricStream

Defining Governance

The governance process within an organization defines and communicates corporate principles, key policies, risk appetite, and oversight frameworks, and evaluates business performance within the context of defined guidelines and principles. Key elements that constitute a governance program include:

- **Risk Philosophy and Appetite:** Corporate governance establishes the risk philosophy for the company. This includes defining risk appetite, rationalizing and monitoring risks, and identifying core areas where the company is willing to retain risks in order to generate expected targeted returns. Streamlining the decision-making process based on risk appetite ensures the integrity and provides a degree of confidence necessary for the organization.
- **Business Ethics and Compliance:** The implementation of an ethical corporate culture and corresponding policies help support overall corporate governance and establish business excellence.
- **Corporate Policy Compliance:** Corporate policy governance optimizes business culture

Gaurav Kapoor
Chief Operating Officer
MetricStream

"Pervasive GRC is MetricStream's vision for the future, representing our desire to help organizations build strong, risk-aware cultures, and to ultimately enable individuals, businesses, and governments to thrive on risk."

- *Responsible for sales, marketing, customer advocacy, and partner ecosystem*
- *Launched ComplianceOnline.com, a leading online GRC community*
- *Bachelor's degree, Technology, Indian Institute of Technology (IIT)*
- *Business degree, FMS, Delhi*
- *M.B.A., Wharton Business School, University of Pennsylvania*

Mr. Kapoor can be e-mailed at gaurav.kapoor@execblueprints.com

and ensures compliance with expected codes of conduct.

- **Business Performance Reporting:** Business performance reporting such as balanced scorecards, risk scorecards, and operational controls dashboards keep boards of directors and senior management informed about all matters related to business performance, compliance, and risk. This insight also manages the expectations of internal and external stakeholders, such as suppliers, employees, customers, vendors, strategic partners, government and regulatory agencies, analysts, investors, and the general public.
- **Corporate Social Responsibility (CSR):** As the requirements for CSR and sustainable growth become progressively more demanding in their degree of transparency, reliability, and ability to be audited, enterprises are creating and enforcing CSR initiatives as a part of their corporate governance to establish an enterprise infrastructure — resources, budgets, planning, IT support — which reinforces these programs.

Risk Management

New and emerging risks are inundating business, and we now live in an era of global supply chains, outsourced labor, virtual IT infrastructures, cyber-warfare, insider trading, rogue employees, increasing regulatory mandates, stakeholder activism, and more. All organizations need to proactively identify and manage risk, whether it is financial, operational, IT, or brand- or reputation-related. Doing so can help prevent reactive and costly crisis management.

All employees have ownership for risk management. A comprehensive risk management program includes:

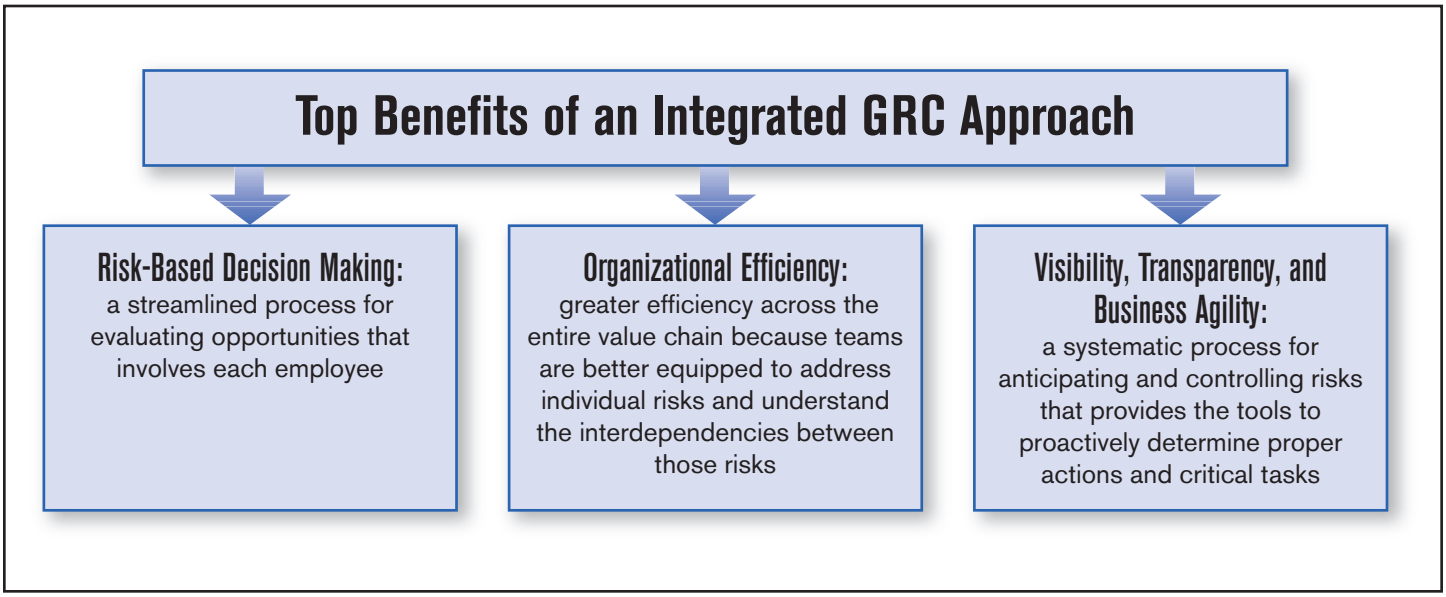
- **Identification:** This entails performing necessary walk-throughs, asking the right questions at the right time, observing key risk management components, assigning appropriate personnel at all levels, and promoting strengthened governance.
- **Analysis:** Teams determine how to address the key risks in the most effective and cost-efficient manner by identifying controls, estimating costs, assessing the degree of risk reduction, and then determining which controls to implement. The output of this process is a clear and actionable plan to control or accept each of the top risks identified in the risk identification phase.
- **Implementation:** During the implementation process, the correct treatment for each risk is chosen and implemented. Risk managers create and execute plans based on the list of control solutions and deploy the requisite tools, processes, and frameworks. This takes place throughout the project cycle.
- **Verification:** Organizations should estimate their progress with risk management as a whole. Verification introduces the concept of a "Risk Scorecard." Implementation efficiency is measured using key performance indicators (KPIs), like percentage of revenues

Expert Advice

Role of Technology Technology can provide a wide range of easy-to-use applications that enable a systematic approach to defining and managing GRC initiatives through sustainable and integrated processes. Technology can enable organizations to do the following in a more effective and efficient manner:

- Drive more sound and strategic decision making through a centralized view of risks that are aligned to business objectives
- Integrate risk and compliance management with business planning and decision making
- Identify opportunities for performance optimization through better risk management
- Reduce risk exposures through early detection, better mitigation, and real-time visibility
- Protect shareholder value and strengthen brand and reputation with robust governance practices
- Improve productivity and resource utilization with streamlined processes and rationalized controls

MetricStream is a fast-growing company that not only provides these effective and efficient solutions to the market, but also uses its own solutions to manage GRC internally.



saved due to early mitigation of risks, revenue increases as a result of innovation in risk management, and the risk exposure amount against the total project value.

- **Monitoring:** Monitoring involves repeating the aforementioned processes regularly and keeping risk information current. It is critical to optimize a risk management strategy, because it verifies existing processes, implements corrective action plans, and streamlines the remediation workflow.
- **Decision Analytics:** Based on risk data aggregation across the enterprise, it is important to contextualize the information to drive decision making that is more accurate, faster, and context-driven. Given that stakeholders are demanding decision making at a more accelerated pace in today's business environment, it is important that GRC information is provided at the point of decision making rather than ex post facto. A good GRC solution will allow for that.

Regulatory Compliance

As companies race to meet regulatory deadlines, the initiatives to comply with these regulations typically begin as a project, consuming significant resources. Meeting deadlines often becomes the most important objective. However, compliance is not a one-time event — organizations today realize they need to turn compliance into a consistent and repeatable process, resulting in lower costs than for the first deadline. When an organization is faced with simultaneous deadlines, a streamlined process for managing compliance is critical. Technology can help make compliance repeatable, collaborative, and sustainable by streamlining efforts, maximizing resources, eliminating redundancies, and reducing costs. A comprehensive regulatory compliance program includes:

- **Document and Process Management:** Most enterprises require their chief compliance officers (CCOs) to follow a process around risk documentation to ensure successful compliance and risk management. The examples of information gathered include risk management plans, assessment reports, handling methods and techniques, and metrics for monitoring risks.
- **Define and Document Controls:** CCOs define and document the control activities that occur throughout the organization, at all levels and in all functions, including approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and the segregation of duties.
- **Monitoring Controls:** Control systems need to be monitored. This is a process that assesses the quality of the enterprise's performance over time, and is accomplished through ongoing monitoring activities and evaluations.

- **Disclosure and Certification:** In GRC, parlance disclosure and certification are the benchmark settings that endorse adherence to requisite compliance and quality mandates. CCOs often rely on certificates and endorsements by the managers and CIOs, as it increases accountability across the processes.

Integrating GRC Management

Many organizations find themselves managing their GRC initiatives in silos. However, as risk and compliance initiatives become more intertwined from both a regulatory and organizational perspective, manifold systems cause confusion due to duplicative and contradictory processes and documentation, resulting in increased business risk. The redundancy of work, as well as the sheer expense of maintaining multiple point software solutions, significantly raises the cost of compliance and risk management.

To address the above requirements, taking a broader and more integrated approach is necessary. This value-add principle is being embraced by a growing number of leading organizations throughout the global business community. An integrated GRC framework can increase compliance effectiveness and reduce the cost of compliance, while aligning GRC initiatives centrally with corporate governance and reporting.

While the value of an integrated GRC program is largely understood in today's business world, most organizations still struggle when it comes to the steps required to build a truly pervasive GRC program that spans the entire organization. Different divisions within a single organization often have diverse GRC programs and processes that operate separately and in silos, rather than working in tandem with one another. To avoid this, organizations must focus on building and implementing an integrated GRC solution that enables the enterprise to manage the entirety of its GRC initiatives on a single and central platform.

Dangers of a Siloed Approach to GRC

A siloed approach often leads to process redundancies and consumes far more time, cost, and effort than required. It also increases the likelihood that an organization will not be able to provide management with the information they need for decision making, hence increasing their overall business risk. The following list includes additional dangers organizations may face with a siloed approach:

- **Process inefficiencies and high costs:** A siloed approach hampers visibility of risks and controls, and their relation to business processes, resulting in inconsistent standards and redundancies around risk and compliance management efforts. Tools such as spreadsheets and e-mails require significant time, coordination, and laborious processes, all of which heighten the risk of manual errors.
- **Lack of collaboration:** It is risky for companies to have several business functions and/or subsidiaries that function independently, each with risk and compliance initiatives that are managed in separate systems with assorted processes. This leads to very little, if any, collaboration and information sharing among the entities and inevitably results in duplicate risk or compliance assessments.
- **Limited transparency:** Managers need a clear view and steady stream of accurate and reliable information in order to proactively identify and resolve vulnerabilities. With a siloed approach, they may have to rely on isolated and manually prepared insights from each business entity, making it difficult to gain a consolidated view at the enterprise level.
- **Lack of centralized documentation:** As companies grow and expand their operations around the world, they are required to provide significant documentation including control assessments, regulatory information, internal policies, and audit reports. When these documents are not stored in a central location, search and retrieval becomes extremely challenging.
- **Insufficient reporting to support decision making:** Without unified reporting, managers have difficulty compiling the required information quickly, and in the desired format. It is also challenging to merge large sets of data on processes, risks, and controls at various levels of granularity to provide value-added information and insights to various stakeholders that

can be used to drive business performance.

The Team Behind the GRC Strategy

A successful GRC program integrates with the company culture, mission, values, and ethical standards. Compliance isn't just about following rules; it is also about corporate behavior and corporate citizenship. Professionals across the enterprise, including chief risk officers and chief compliance officers, have become an important nexus of GRC insight across the organization. The following are important job functions that will also play a critical role in building and leading a world-class GRC program across the organization.

Board and Corporate Governance

Corporate governance is the system by which companies are directed and controlled (Cadbury Committee, 1992). Its purpose is to optimize resources to promote accountability and efficiency within the corporate structure. The board of directors sets the company's corporate governance, establishing and promoting policies for management and employees of the corporation. Companies require a flexible framework for streamlining governance programs, ensuring corporate governance compliance, and improving accountability and communication, which facilitates adoption of corporate governance principles and best practices.

Risk Management and Assurance

Risk manager roles have evolved from just reducing and managing a predetermined set of risk exposures to being central players who respond to existing and emerging risks. They identify where and when the company should be willing to retain risk in order to seize growth opportunities and generate returns. This ties risk management and assurance to business performance, fundamentally changing the practice of risk management from an exclusively centralized function to a federated, top-down approach that is aligned with business objectives and reporting, whereby assessments are distributed to lines of business for ownership, execution, and accountability.

Compliance and Ethics

Compliance and ethics managers are entrusted with ensuring that an organization has the processes and controls to meet the requirements imposed by governmental bodies, regulators, industry mandates, or internal policies. Compliance managers are now focusing on effective rationalization of controls to provide a clear, unambiguous process for compliance management, and to ultimately deliver a single point of reference for the organization.

Audit Managers

Audit managers are critical contributors to business performance because they provide an independent assessment and overview of the state of the business. They are accountable for monitoring risks and ensuring compliance across organizational silos, which requires a common framework for all types of audits, and determines priorities through an enterprise-level risk-based approach — not by departmental and tactical imperatives.

Finance and Internal Controls

The bar for finance executives and internal controls managers has been raised in key areas such as corporate governance, risk management, and compliance. They must re-engineer finance and controls processes to address and focus on those higher value-added activities that drive business performance, while also helping to strengthen process controls, manage risks, and meet regulatory and compliance requirements. The CFO is emerging as the logical epicenter of an integrated approach that demonstrates rigor and discipline in balancing the demands of boards, analysts, regulators, shareholders, customers, and broader market forces.

Regulatory Affairs

In regulated industries like health care, life sciences, energy, food, and banking, regulatory affairs serve as the primary communication link between the company and the regulatory agencies. They are responsible for staying current with the increasing scope and complexity of regulations, and assist various functions within the company in interpreting and understanding these complex laws and regulations.

Policy Management

Regulators and auditors are keen to know how the company defines and maintains its policies across various aspects of the business and its operations. A policy manager helps define, manage, update, and report on the status of these policies, and is also responsible for ensuring that the policies are scripted correctly so the results match the intended outcomes. A flexible framework that can streamline the creation and management of polices and also facilitate accountability, improve communication, and provide sound

reporting and analytics is crucial for policy managers.

Legal Counsel

Legal counsel is required to act with absolute integrity in assuring that the company is operating within the bounds of the law. They need to understand the various aspects of the business and proactively communicate any associated legal issues to management. Legal counsels can add tremendous value by having clear visibility and ensuring a centralized view of the relevant legal information to provide context and flag potential risks.

Quality Management

Quality managers are focused on ensuring that the company's products and services meet or exceed the expectations of its customers. They are also responsible for leading a sustainable program that improves quality, while also maintaining stringent delivery schedules and the price of the product or service. In managing such a complex set of activities and processes, quality managers need to have real-time visibility to establish sound quality processes throughout their supply chain and distribution network.

IT Security and Governance

IT security and governance professionals are tasked with everything associated with ensuring, establishing, and enforcing security policies, standards, and procedures. IT security managers continuously monitor all components of the IT infrastructure for compliance adherence and security threats, and take appropriate remedial action as necessary. They also conduct IT risk analyses and assessments and ensure adequate remediation plans are in place to mitigate the risks. An established governance framework to manage all IT-GRC-related activities can help IT security professionals in manage IT governance and related issues, such as policy, risk, compliance, audit, and incidents in an integrated manner.

Top Benefits of an Integrated GRC Approach

The top benefits of an integrated approach to GRC includes risk-based decision making; organizational efficiency; and visibility, transparency, and business agility.

- **Risk-Based Decision Making:** An integrated GRC program allows for efficient risk-based decision making and provides a streamlined process for evaluating opportunities. Each employee plays an active role in the organization's risk management efforts.
- **Organizational Efficiency:** An integrated GRC program provides various benefits, including greater efficiency across the entire value chain, by providing the top-down coordination that is necessary to make the financial and non-financial functions of an organization work as intended. An integrated and collaborative team is better equipped to address the individual risks facing the company and understands the interdependencies between those risks.
- **Visibility, Transparency, and Business Agility:** An integrated approach enables transparency, gives management a systematic process for anticipating and controlling risks, and provides the tools to proactively determine proper actions and critical tasks, helping to reduce unfavorable or unacceptable performance variability. As the current financial environment continues to change at a rapid pace, an integrated GRC program manages and evaluates assumptions in the current business model, and assesses the effectiveness of strategies for new business models. By enabling decision makers to identify and assess alternative future scenarios, they are in a better position to lead the company to long-term and sustainable success.

Creating a GRC Roadmap

While there is no "one-size-fits-all" approach to integrated GRC, the GRC framework should not merely lead to compliance; it should also provide the organization with mechanisms to better understand and manage the nature of their risks. A robust GRC framework is comprised of the following components:

- **Risk Governance:** It is essential that the management team provide clear guidance on risk appetite or tolerance, policies, and processes for day-to-day risk management.
- **Structure:** When designing an integrated GRC structure, the organization's overall risk scenario serves as a guideline to establish a standard reporting format for business risk reviews. Establish a hierarchical structure that integrates the risk management function into existing processes, leverages current risk and compliance

processes, and capitalizes on existing capacities and capabilities.

- **Implementation:** An ideal integrated GRC management program enables organizations to efficiently identify, assess, and report GRC-related information including risk and control self-assessments, regulatory assessments, loss data collection, and more. The comparisons between different sources of information on a consistent basis leads to the ability to carry out audit activities, assess risks, draw more powerful conclusions, and prepare stronger recommendations for risk mitigation.
- **Responding to Events:** When an event is identified and assessed, a decision is made to identify the appropriate response. The next step is responding to the identified risks, which involves establishing the desired results by first defining the objectives and expected outcomes for ranked risks; classifying and analyzing options to minimize threats and maximize opportunities; choosing a strategy to apply decision criteria; and then applying the precautionary approach/principle as a means of managing risks.
- **Ensuring Continuous Learning:** Continuous learning is fundamental to sound and proactive decision making. It contributes to better risk and compliance management, strengthens organizational capacity, and facilitates the integration of GRC management into the organizational structure.

The Future — Pervasive GRC

Globalization, virtualization, mobility, social networking, and hyper-connectivity — these trends have taken the world by storm while introducing new risks and new regulations that businesses are just now beginning to comprehend. The future belongs to well-governed, compliant, and risk-intelligent organizations — those that actively embrace pervasive GRC. Pervasive GRC is about bringing together people, processes, and data in a unified framework through cohesiveness and integration. The technology that supports it must also be defined by these same characteristics.

A truly unifying and pervasive GRC technology can help organizations build a centralized and transparent GRC ecosystem. It can support an enterprise-wide culture of GRC awareness and accountability by enabling and empowering each employee and business function to manage their risk and compliance responsibilities independently, while simultaneously rolling up data from across the enterprise to provide a complete top-level GRC perspective. Technology can be used to support gathering mountains of data from across the ecosystem, processing this data in real-time, and applying advanced analytics to help organizations draw insights, foresights, and predictions, and align their business strategy accordingly.

About MetricStream's GRC Solutions

We are now living and doing business in a mobile, social, and global world that has witnessed an explosion of new and emerging risks, sweeping regulatory oversight, the rising importance of reputation, intertwined third-party relationships, and more. MetricStream's Governance, Risk, and Compliance (GRC) software solutions are empowering employees and organizations of all sizes around the world to become more risk-aware, more compliant, and better governed. MetricStream's holistic, integrated, and collaborative approach to GRC allows organizations to proactively identify and respond to domestic and global events and trends much faster. By putting a unified enterprise-wide structure in place to manage GRC, organizations can make decisions faster and feel more confident that those decisions support the organization's short- and long-term objectives, provide competitive advantage, and drive sustainable growth. ■

Valeh Nazemoff

Senior Vice President, Acolyst

Defining GRC

The term "GRC" (which stands for governance, risk management, and compliance), generally means something different to IT, finance, marketing, and other departments within an organization. However, it should collectively reflect the collaboration and communication flow of people, information, processes, and technologies across the organization. The main goal of an effective GRC strategy should be to establish a framework so that the organization is not consistently reacting to incidents and events such as regulatory changes, but instead has a systematic process in place for managing such modifications. A GRC strategy enables an organization to be proactive in managing variations and transformative occurrences.

The main goals of an effective GRC strategy should be to establish a framework so that the organization is not consistently reacting to incidents and events such as regulatory changes, but instead has a systematic process in place for managing such modifications.

Valeh Nazemoff
Senior Vice President
Acolyst

Process and Approach

With respect to how the three components of GRC should be addressed, first let's distinguish the separation between process and approach. Once the processes have been defined and the people, information, and technologies that will be involved are determined, then the approach is authorizing who does what, when, how, where, and why. This is critical in executing a proper GRC framework within the organization.

The proper roadmap and assessment should help you determine which data, processes, and technologies should go with an order of priority in a timeline, and a step-by-step documented approach. For example, look at the data. How does the data impact users, information, processes, and technology? Map out current governance practice and make sure to include focus on the business's objectives and initiatives.

This documented approach should also include and reflect the following:

- Compliance
- Business process impact
- Impact to the business (dealing with scheduled and unscheduled downtime)
- Risks (financial and non-financial)
- Criticality of the information
- Collaboration of the information
- Cost analysis
- Structure (ex: which data remains in-house versus on public cloud, private cloud)

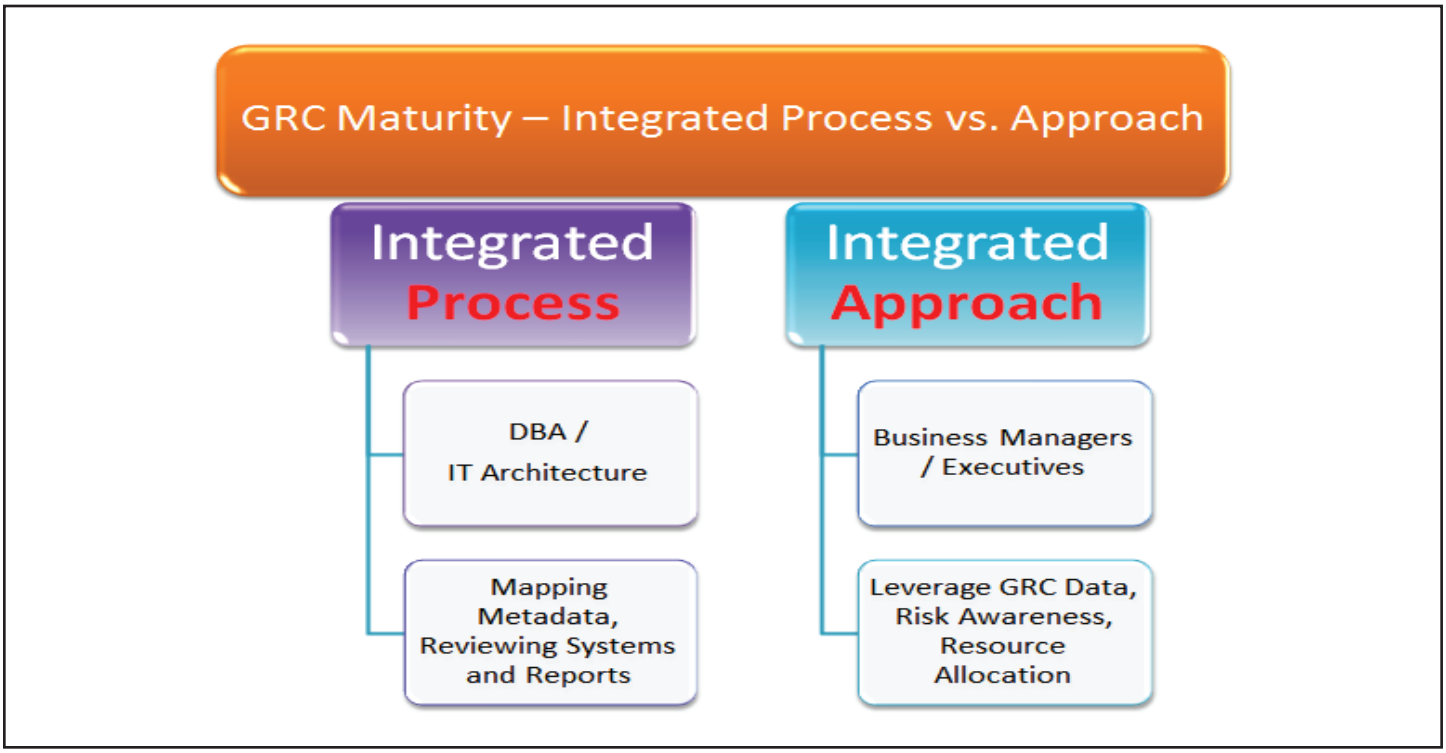
Once you have your plan in place, data model it to help you visually see the input and output of data across the different users and processes that will be impacted. When your data is modeled, prototype using simulated data. Later, at the user testing stage, the users can help you with additional feedback through visual illustration of

Valeh Nazemoff
Senior Vice President
Acolyst

"Using a GRC framework system, an organization can oversee risks, conduct audit and control testing, manage policies and programs, monitor issues and incidents, and continually map to improve processes and handle changes effectively."

- *Guides executives in business process improvement initiatives*
- *Led project teams in collaborations with IT, legal, financial, and other departments*
- *Undergraduate degree in psychology focusing on organizational behavior*
- *Two M.B.A.s (e-Business and International)*

Ms. Nazemoff can be e-mailed at valeh.nazemoff@execblueprints.com



how the data, processes, and technologies will operate and the ways the users will be impacted.

Establishing Integration

Establishing integration helps reduce the overall risk to the organization because risks are codependent and shared across the organization. With an integrated GRC, executives and board members have the visibility needed to make critical decisions. Most importantly, they will be able to communicate the same consistent message and thus allocate resources easily.

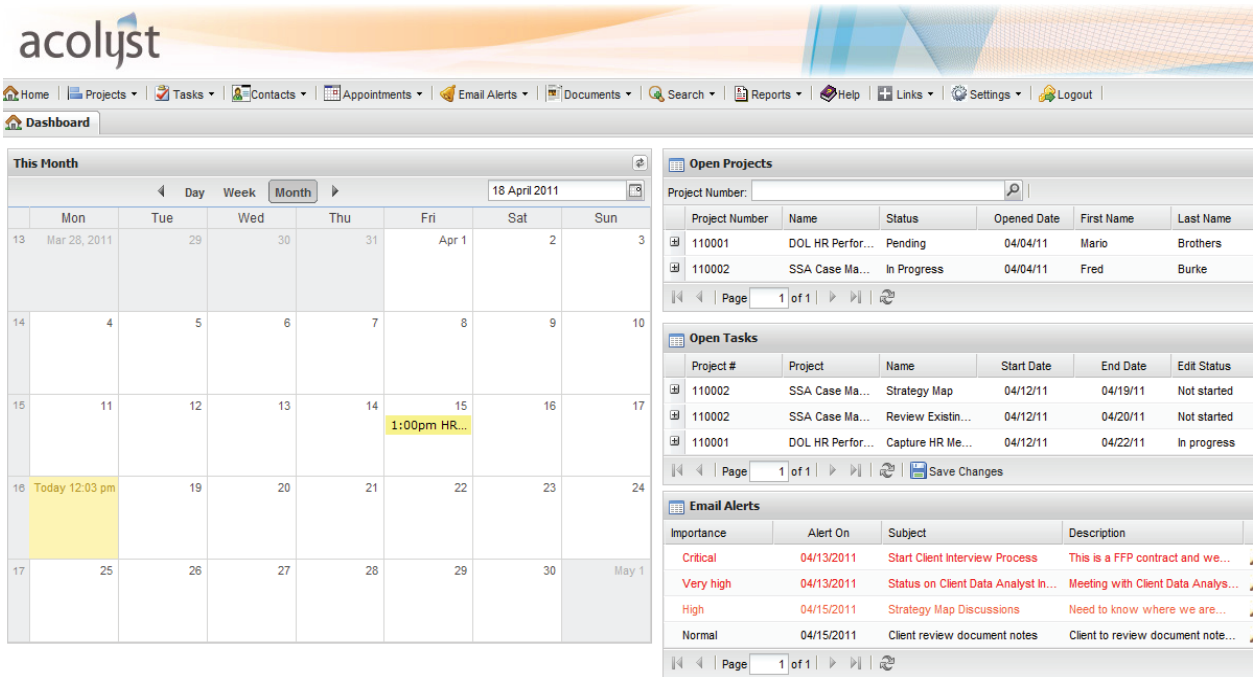
When trying to achieve an integrated approach to GRC, break it down into phases and steps. Identify the enterprise target or the gap analysis from where you currently are to where you need to be and then piece it into sections. For example, do not implement the GRC framework across your enterprise all at once. Instead, pick a few departments then add another department to the mix, and so on. The GRC framework is a cyclic approach that needs to be consistently reviewed, managed, and modified. As business requirements change, regulations change, audit reports change, and technology changes (i.e., social media, mobility, big data, cloud computing, and so on), GRC requirements will evolve and change as well.

The Risks of a Silo

A siloed approach brings several risks, including duplication in efforts, and a lack of communication between those who are ultimately responsible and accountable, specifically the executive team and the board of directors. The lack in communication ends up slowing down company programs and initiatives that need to be implemented since the company cannot keep up with new and improved interaction and engagement of requirements. Often, if a GRC approach is not mature but rather still exists in silos, then decisions will be based on partial information. This can be a major risk and can negatively impact the organization. As a result, when incidents, such as a data security breach, or external changes like regulatory or audit reporting occur, the organization must react immediately.

This exertion of excess energy, time, resources, and money is not the best way to approach the problem. Instead, the company should have been proactively taking charge to ensure the organization, as a whole, is compliant. With a siloed GRC approach, how can the business's goals, objectives, and strategic initiatives be in sync? A common dialogue and consistency of language across the organization go missing. This limits

Acolyst's GRC & Legal Information Management System



collaboration, association, and integration of data.

Top Benefits of Integration

An integrated approach brings harmony, synchronization, and coherence. The top three benefits of an integrated approach to GRC are:

- Collaboration
- Centralized risk response and readiness
- Consistency and confidence in data and information

With an integrated approach, the following are examples of major issues and obstacles that can be avoided:

- Siloed domain focus (ex: Sarbanes-Oxley)
- Reporting issues (ex: external auditors)
- Duplication of resources assigned
- Redundancy of work causing unnecessary costs
- Inconsistent security policies, access to data/information
- Lack of visibility into the areas of risk

Formal Documentation

Some of the formal documentations and procedures that have been developed for my clients include:

- Organizational communication matrix
  - Designated executive sponsor(s), departmental executives, board members, liaison officers, and accountable and responsible parties (i.e., compliance officers)
- Informational architecture design
  - Understanding the flow of data across the enterprise
  - Data modeling, capturing data source information, data standards, definition, metadata (common language), accessibility (security), mapping spreadsheets
- Internal and external formal Service Level Agreements (SLAs)
- Gap analysis documentation
- Strategy roadmap document
  - Includes the types of reporting and for who
- Training plan

Bring Your Own Device (BYOD)

There have been several developments that have influenced our approach to GRC. The manners in which we communicate and behave are changing dramatically. For example, we had to implement an organizational policy revolving around Bring Your Own Device (BYOD)[1] and mobility in the workforce to enhance productivity and business intelligence. This type of reporting has influenced the need for a mature GRC framework.

Also, over the past three years, the need for additional security to mitigate risk has increased. The personal data on personal devices needs to be blocked and added security must be implemented for the mobile business applications. However, a BYOD program can increase performance and boost employee morale, productivity, and collaboration because personal devices can allow for quicker response time to information, requests, and approvals.

The U.S. Federal CIO, Steven VanRoekel, issued the Digital Government Strategy[2], made publicly available on August, 23, 2012, to serve as a government-wide BYOD toolkit. The toolkit contains good starting-point considerations that government agencies and non-government agencies can use for implementing a BYOD program.

Working as a Team

With an integrated GRC approach, there is alignment between various business lines, operations, IT, HR, finance, legal, and more. Therefore, designated key resources should be assigned from each department impacted in developing and implementing an enterprise GRC strategy. These individuals will be part of a steering committee and serve as champions to the overall initiative. Depending on the size and complexity of the company, it is best if various liaison officers are assigned. As business needs, regulations, compliance, and demand of the market rapidly change, the executive team and board members are ultimately responsible and accountable. As a result, we need to ensure that proper communication, analysis, and changes are implemented impacting the people, information, processes, and technologies involved.

Expert Advice

The Year Ahead In the coming year, we plan on promoting the benefit and value of establishing internal Service Level Agreements (SLAs), which help departments get into the habit of formally documenting; agreeing to terms and conditions, measures, metrics, key performance indicators (KPIs), and key risk indicators (KRIs); setting targets; and, most importantly, allowing the departments to understand the needs of the others. Establishing internal SLAs promotes effective communication – eventually – across the organization, improves actual compliance, establishes audit requirements, improves reporting and insight, allows for creativity, and promotes change.

Calculating ROI

Generally key drivers generate the greater need for a strategic GRC. This in turn helps justify the ROI. Here is the list from my whitepaper[3]:

- To support BI/data warehousing initiatives
- To support a Master Data Management (MDM) initiative
- To facilitate the migration of legacy data
- To meet compliance and legislative requirements
- To reduce corporate risk
- To improve corporate flexibility and business agility
- To support operational software upgrades (e.g. ERP, CRM, etc.)
- To reduce costs
- To support handling of mergers and acquisitions

However, some of the basic arguments for GRC that can be used for measuring ROI would include:

- Reduced audit costs due to fewer resources and integrated systems/reporting
- Faster response time to resolve issues and risks
- Fewer incidents and fines
- Better and more informed decision making

Top Challenges

Based on lessons learned and best practices, some of the top challenges that exist in developing an effective GRC approach are:

- Transitioning departmental executives from a siloed to an integrated GRC approach, i.e., adopting the culture and change

- Making sure everyone complies with regulatory and government mandates
- Shifting from the siloed use of technology to an integrated use, especially integrating the flow of processes
- Managing change through the assignment of who is responsible and accountable for changes during transformation to an integrated GRC approach
- Coping with fear that jobs will be lost — especially if legacy systems will be replaced

In order to overcome these challenges, there should be an executive sponsor high up in the chain who blesses an integrated GRC approach. There should be a steering committee, a voting policy, and a mediator in place. For example, with personnel policies, the executive sponsor must make sure that HR releases an appropriate and sufficient amount of data, and does not withhold information to slow down the progression of an integrated GRC strategy.

Global GRC Benefits

An integrated GRC strategy can benefit a global organization by focusing on similarities rather than differences. However, when working across international locations, geography, legal, and cultural differences should be considered. Take into account the U.S. Foreign Corrupt Practices Act of 1977 (FCPA) where foreign government policies and procedures vary by country. The FCPA prohibits U.S. companies, their subsidiaries, officers, directors, employees, and agents from making corrupt payments or favorable treatment to "foreign officials" for the purpose of obtaining or keeping business. The complexity of following FCPA and foreign regulations makes establishing controls and testing costly. In turn, organizations struggle with implementing controls to support internal FCPA policies (i.e. Sarbanes-Oxley, company's code of ethics translated into multiple languages, among others). Some companies believe that by having anti-corruption and -bribery policies in place, they will remain in compliance. However, the FCPA requires more. The same is true for other regulations and mandates that need to be considered.

Establishing an integrated GRC framework gives a company visibility and insight, plus the ability to reduce cost and exposure to violations, and increased control over remote operations and employees. ■

Featured links

1 "Bring Your Own Device" available at: http://smarterprise exchange.com/groups/cloud/blog/2013/02/13/bring-your-own-date-byod-to-the-governance-dance-ball

2 "Digital Government Strategy" available at: http://www.whitehouse.gov/digitalgov/bring-your-own-device#introduction

3 Valeh Nazemoff's white paper available at: http://acolyst.com/wp-content/uploads/2013/04/Acolyst-Data-Governance-White-Paper_Final.pdf

Ideas to Build Upon & Action Points

I. What Is "GRC"?

Companies have been doing governance, risk management, and compliance (i.e., GRC) for a long time. The concept of GRC, however, is relatively new — and it denotes much more than the simple definitions of the terms listed in the acronym. As described in this ExecBlueprint, GRC "represents an integrated approach to the governance, management, and assurance of performance, risk, and compliance." In other words, it is about establishing a holistic way to bring together people, processes, and data to understand and manage the organization's risks. A fully developed GRC strategy should accomplish the following for its organization:

- Provide unified vocabulary and taxonomies for information
- Establish common repositories for data, documents, and information
- Create standardized procedures and templates for policies, trainings, etc.
- Ensure regular and consistent communication between strategic decision makers and other key staff

II. The Bottom Line

A well-executed GRC strategy includes scorecards that document the costs associated with taking and mitigating risks, along with other business performance indicators. While measuring the ROI of GRC activities can be difficult, you can compare the efficiencies gained by allocating resources based on these clear metrics versus your intuition. To assess the value of your GRC strategy, you can also explore the following questions:

- Have you experienced a decrease in safety incidents and liabilities?
- Have your integrated systems and reporting processes resulted in reduced audit costs?
- Have you reduced your response time to resolve issues and risks?
- Have your innovations in risk management resulted in increased revenues?
- In what ways have improvements in corporate flexibility and business agility resulted in the more successful execution of business initiatives?

III. Must-Have Benefits of a GRC Model (and Pitfalls of a Siloed Approach)

New and emerging risks are now inundating organizations: globalization, virtualization, mobility, social networking, and hyper-connectivity all present new issues (in addition to opportunities) that must be managed in a well-governed, compliant, and risk-intelligent way. An organization with a strong GRC capability is better positioned to identify risks and compliance requirements and, thus, can engage in effective strategic planning that is more likely to result in the attainment of established goals. Specifically, GRC can benefit organizations by:

- Enabling leaders to understand the organization's risk appetite and strategic goals, so that risk can be leveraged without exceeding established thresholds and tolerances
- Providing top-down systemic processes that give management the information and tools they need to address risks and respond appropriately to events
- Improving the organization's response to new regulations through the institution of streamlined compliance processes
- Facilitating agility so that the organization can shift direction to avoid threats, grasp opportunities, and recover from adversity
- Empowering employees to take a more active role in managing their risk and compliance responsibilities, sharing their data, and utilizing real-time risk intelligence

An integrated GRC approach can also help organizations avoid the following pitfalls of a more siloed approach to these activities:

- Lack of communication between managers, executives, and the board of directors concerning areas of risk, resulting in decisions based on partial information
- Inconsistency in standards around risk and compliance management systems and tools — and in application of policies relating to security and access to data and information
- Lack of centralized documentation, including control assessments, regulatory information, internal policies, and audit reports
- Duplication of effort, resulting in unnecessary costs and increased likelihood of errors
- Reactive responses to incidents (such as data security breaches or regulation changes)

IV. The Golden Rules for Developing a Sound GRC Framework

Adopting a broader and more integrated approach to governance, risk management, and compliance requires taking numerous steps — and companies should not attempt to execute them simultaneously across the company. Rather, they should begin with a core group of departments, and work outward. The Open Compliance & Ethics Group (a nonprofit think tank) has issued open-source standards for establishing a GRC framework that are available at oceg.org. The process includes:

- Attaining unqualified support from senior leadership, and instituting a steering committee to drive the process
- Establishing a "risk philosophy" for the company that involves defining the risk appetite, monitoring risks, and identifying core areas where the company is willing to retain risk to generate expected returns
- Linking risk management to strategy development and resource prioritization at the highest levels of the organization
- Defining the organizational structure so that risk and compliance become everybody's business
- Cultivating a mindset that uses risk to inform — and share — objectives, priorities, and plans across the company, rather than in siloed groups
- Determining the data, processes, and technologies that will be necessary to execute an effective GRC framework
- Developing procedures for every line of business to identify and evaluate risk, develop and implement response plans (capitalizing on existing capabilities where possible), and monitor progress
- Informing vendors and consultants of the company's new approach to risk and compliance
- Acknowledging that implementing a GRC framework will involve a cyclic approach involving reviews and modifications

V. Essential Take-Aways

While the GRC model will necessarily evolve in response to changes in business requirements, government regulations, auditing foci, and technology, it will always need to support organizations' efforts to comply with applicable standards and manage risk appropriately so that business objectives can be achieved. Key components of an effective GRC strategy are:

- Supportive senior leadership and board of directors that exercise due diligence in establishing governance processes to ensure compliance, accountability, and communication
- Enterprise-wide independent roles for chief compliance officers, chief risk officers, audit managers, policy managers, and legal counsel
- Decision analytics that are based on an aggregation of risk data across the enterprise
- Companywide document and process management, including risk management plans, assessment reports, service level agreements, and handling methods and techniques
- Risk managers, compliance and ethics managers, and compliance and risk committees for each line of business to ensure communication and coordination of activities
- Robust department-level risk management programs that include identification and analysis of risks, implementation of solutions, and monitoring of results
- Effective information management systems that support the flow of information and decisions up and down the chain
- IT security teams that assess risks, develop and enforce policies and procedures, continuously monitor the IT infrastructure for threats, and respond to incidents ■

10 Key Questions and Discussion Points

1. What does "GRC" mean for your company? How does your organization approach the components of governance, risk management, and compliance? What are the main goals of an effective GRC strategy?
2. How can an organization achieve an integrated approach to these strategic areas? Why is it important to establish this integration? What are the main risks of a siloed approach?
3. What formal documentation or procedures have you developed in terms of your GRC strategy? What purpose does this documentation serve?
4. Who are the "main players" in developing and implementing a GRC strategy? Why should these individuals be included in the process?
5. What role does technology play in your GRC approach? Do you use specific GRC software? What are the benefits or drawbacks of this technology?
6. What trends and industry developments are influencing your approach to GRC? How have these trends changed in the past three years? What trends are likely to influence future GRC approaches?
7. What are your best practices for creating an effective GRC roadmap? What key components must be included?
8. What role can vendors and consultants play in designing an effective approach to GRC? What are the main components of a successful partnership? What key questions should be asked when forming these partnerships?
9. How can you calculate the ROI for GRC strategies and solutions? What is measured?
10. What are the top challenges that exist in developing an effective GRC approach? How can organizations overcome these challenges?