The ABCs of GRC

This column accompanies the illustration on the facing page fold-out, which is part of OCEG's GRC Illustrated Series. To download a copy of the illustration and others in the series, visit the OCEG website at www.oceg.org/resources or go to www.complianceweek.com and select "GRC Illustrated" from the "Topics" pull-down menu on the toolbar.

By Carole Switzer

OCEG, the think tank that defined the business concept of GRC, has long talked about GRC as the set of capabilities that enable an organization to reliably achieve its objectives, while addressing uncertainty and acting with integrity. This outcome is what we call Principled Performance, and it demands a mature, integrative approach to governance, risk management ,and compliance, the component parts of GRC. The value of mature GRC capabilities can be summed up through another acronym—ABC: Aware, Bespoke, and Confident. And while these are not the only attributes of effective GRC, together these three offer the opportunity for greater success that most organizations have failed to grasp, at least up until now.

Business today faces challenges like never before. The advances in communication, information flow, and technology of the past decade offer benefits, but also create complexity. The velocity of change, not just the speed, is overwhelming and virtually impossible to contain. And none of the change is linear; it is always layered, multi-directional, constantly shifting, and complicated by interaction. The ABCs of GRC are more important now than ever before.

A is for Aware

To have strong governance and business leadership that drives successful strategies and outcomes, you have to learn some things that you can only learn by being aware:

- aware of the external business, societal, geopolitical, and physical environment in which your organization operates,
- aware of the internal business context including culture, resources, stakeholders, and goals, and
- aware of the potential risks and requirements that may present threats and opportunities.

B is for Bespoke

To prevent adversity and grasp opportunities with agility and resilience, you must align customized processes and controls to your own objectives, risks, and compliance needs—as well as to your organizational structure and culture—so they fit your business given the context in which it operates. As my British colleagues would say, you need a bespoke approach that is tailor-made and aligned to your own needs, not an off-the-rack template that is one size doesn't fit any.

That doesn't mean building every technology in-house, quite the contrary. It means analyzing what is possible then carefully selecting what you need and rejecting what you don't as you design and build your ideal set of capabilities. It also means using guidance in the OCEG GRC Capability Model to determine your own ideal GRC organizational structure and your own aligned GRC management actions and controls. By doing so, you can fill gaps, reduce redundancies, smartly apply resources, ensure information quality, and make more informed decisions.

C is for Confident

To gain true competitive advantage, you must perform to the best of your abilities and that requires a high level of confidence that you "know what you need to know" and have planned appropriately to both protect the business and propel it forward. When you fully understand your business risk appetite and tolerance levels, have metrics and triggers established to ensure you stay within those boundaries, and can align your objectives to identified opportunities, you have an advantage.

> "When you have taken the necessary steps to be aware, have implemented bespoke GRC capabilities and have established a comfortable level of confidence, you have advantages that will bear dividends over time.

You are able to act more quickly, take more calculated risk, and define future direction better than those who are basically operating in the dark and "governing by guessing."

OCEG's research has shown that companies with more mature GRC capabilities are significantly more confident that they have the right controls in place to address their risks and compliance obligations. They are more confident that they can take risk and use it to their advantage. They are more confident that they can meet their objectives while addressing uncertainty and acting with integrity. By using the ABCs of GRC, you become a more educated and more capable organization that will continue to evolve and keep up with the changes that are yet to come. ■

COMPLIANCE WEEK

GRC Illustrated

The Journey to Advantaged GRC

As organizations mature their approach to GRC, they transition from a structure of siloed departments and units to a fully engaged business operation where everyone has a part in managing risk, ensuring compliance and contributing to performance outcomes. This leads to greater confidence, agility and resilience - advantages that ensure success.

Compliance Week and the Open Compliance and Ethics Group have teamed up to provide readers with this regular illustrated series on governance, risk, and compliance programs. For information on this series and a downloadable version of this illustration, please go to www.complianceweek.com, and select "GRC Illustrated" from the "Topics" pull-down menu on our toolbar.

DEVELOPED BY OCEG®

WITH CONTRIBUTIONS FROM RSA® The Security Division of EMC

Siloed GRC

- Focus on compliance
- Reporting is disconnected
- Processes are isolated

COMPLIANCE

Did you know we set up six new suppliers in Dubai?

No, that means we need to start review of regulations. Wish we'd heard about this sooner.

Every division has its own policy management system and we can't reconcile the data.

RISK

We've asked key managers to tell us their top risks but they all report differently.

We monitor external changes but the information never gets to the right people at the right time.

We need to know about planned strategic and operational changes earlier to assess risk.

OPERATIONS

ABC Company has the best solutions

WeeBee Software has the best solutions

ACME Corp. has the best solutions

AUDIT

How are we supposed to provide assurance when every department and unit uses different terms and metrics?

It's going to take weeks to reconcile this and find any actionable information.

Managed GRC

- Focus is on risk
- Reporting is coordinated
- Processes are defined

COMPLIANCE

We need to set up company-wide policies and training to address this issue.

This compliance report says our incident levels are higher than other departments but we don't know why.

RISK

This can impact the business, but we can't reconcile the data from different regional divisions to analyze it well.

At least everyone is using the same risk assessment methods now.

OPERATIONS

We've highlighted the top risks and incidents for you.

RISKS

INCIDENTS type location severity

Please tell me how this affects our business plans and current operations. Just knowing our risks isn't enough.

AUDIT

It's easier to complete our audits with the new standard reporting system, but we still can't see the impact on future plans for the business.

It helps that all the units are using the same terminology now.

Advantaged GRC

- Focus is on business opportunity
- Reporting is enterprise-wide
- Processes are optimized

REGULATORY CHANGE
REGION
OPERATIONS
RISKS

OPERATIONAL
REGION
OPERATIONS
RISKS

We help every department review controls when there are regulatory or operational changes.

We're flagging changes that impact operations.

Now we can see how changes in operations might impact our risk tolerances.

Yeah, and we consider our risk assessments and compliance requirements when we make strategic decisions.

We're finally getting an enterprise-wide view.

BUSINESS BENEFITS

THREATS | IDENTIFIED OPPORTUNITIES | COSTS | AGILITY

These reports let us plan and adjust in real time as internal and external factors change.

IMPACTS ON STRATEGY

We're more confident that we can take advantage of risk now.

GRC MONITORING & METRICS

RISK PREDICTIONS > | OPPORTUNITIES > | RELATIONSHIPS >

Our reports show the possible risk outcomes for operational or strategic changes under consideration.

We can advise the board and operations better now.

TRANSITIONING
focusing on repeatable processes

TRANSFORMING
focusing on business operations

{AN OCEG ROUNDTABLE}

The Advantage of Advantaged GRC

Switzer: OCEG has long framed discussions about GRC with the concept that GRC enables Principled Performance—the ability to reliably achieve objectives while addressing uncertainty and acting with integrity. This concept dovetails nicely with the term RSA uses: Advantaged GRC. Would you explain what that means and how it shapes the GRC discussion in companies that embrace it as a driving goal?

Toburen: Advantaged GRC is the most mature state of GRC capability, and it closely aligns with and enables OCEG's goal of Principled Performance in two ways. First, it is at this stage of maturity that organizations are most often looking at opportunities to enhance performance versus the risks and obligations they are faced with. Second, they have created a GRC framework that best ensures their decisions to pursue opportunities that are executed thoughtfully and in accordance with the organization's objectives, policies and procedures, risk and control management program, and regulatory obligations.

As organizations mature their GRC programs, they consolidate information from across silos, develop business context, establish common governance practices to be applied across all business units, and begin to explicitly hold individuals accountable for the ownership of activities and associated risks and risk treatments. This growth in maturity takes the organization from ad-hoc, reactive governance to consistent day-to-day governance. They move from seeking to capturing management efficiencies and enabling best practices, to gaining a fuller understanding of the business context of risk and compliance. By the Advantaged GRC state of maturity, the organization is no longer just seeking to minimize risk taking, but rather looking to understand how taking risk can lead to the exploitation of business opportunities.

Aldrich: Principled Performance and Advantaged GRC are very compatible concepts. As a GRC practitioner, I see common prerequisites for enablement of Advantaged GRC and achievement of Principled Performance: a seat at the table to understand business initiatives, an executive sponsor, consistent risk taxonomy, a mature data management strategy, and a technology solution to facilitate enterprise reporting. Unfortunately, many companies only have a few pieces of the GRC capability pie that prevents them from establishing Advantaged GRC and achieving Principled Performance. However, this shouldn't discourage their quest to reach these most mature levels that truly support their business outcomes.

Switzer: Clearly, the biggest change in GRC over the past decade has been in technology becoming better, cheaper, and easier to implement. How does this change enable companies to mature their capabilities and establish Advantaged GRC?

Aldrich: Today, more companies understand what a GRC program and technology can accomplish. They see the real value it can provide. Previously, many companies had an ill-conceived notion of GRC and how to implement a GRC platform. Over the years, as the capabilities of GRC technologies improved, the GRC implementation best practices improved as well. It still takes an experienced GRC practitioner to successfully implement a GRC technology. It's still not an "out of the box" process. Luckily, we have more people with the "GRC Battle Scars" to successfully navigate complex GRC technology implementations and achieve GRC maturity with a corporation much faster than ever before.

Toburen: Certainly software alone does not make for a good GRC program. GRC software is one of the three legs enabling a GRC program, the other two being people and process. But GRC is about good governance and GRC software is about enabling good governance. Organizations that implement GRC software are making a big commitment that they want to have better governance of risk and compliance. That commitment alone is a huge step toward greater maturity.

We want to see organizations get their programs up and running as quickly as possible so our mantra to inspire everyone to own risk is quite real. It is important to us to provide GRC software that fits the organization's desired level of maturity and as they reach that level, if they decide to increase maturity or extend their GRC scope, they can easily do so by extending the software. In addition, inspiring everyone to own risk means we make it as easy as possible for software users to understand what they need to do, and how to do it and to present actionable information to them that helps them with their day-to-day governance responsibilities.

Switzer: When OCEG ran our first GRC maturity survey 10 years ago, the biggest challenge identified was the difficulty in reconciling disparate information. To the extent companies were focusing on integrating or harmonizing GRC capabilities, the desired goals were largely around ways to reduce gaps and inconsistencies more efficiently. Are these still the primary challenges and goals today?

Toburen: Many organizations have come a long way with their GRC programs over the past several years, but still GRC information accuracy and completeness poses day-to-day challenges with program managers desiring to strengthen their data governance. This is very much an administrative task looking for data that is not current or broken and missing links between records such as risks without controls or business processes without risks.

But the challenge we see most consistently today for organizations just starting out with GRC as well as those with established programs that have had turnover in leadership or key program managers, is the people component of GRC. Closely related to the culture of risk management, this is about getting everyone on board with GRC concepts and strategy and getting them to actually engage in day-to-day GRC. First and foremost this is about the tone from the top, but it also requires a lot of training and reinforcement about what GRC means to the organization and stakeholder accountability for program elements. A nice thing about GRC software and RSA Archer in particular, is that it reinforces the desired engagement with first line of defense business unit managers and second line of defense risk and compliance managers, while providing transparency to third line of defense internal auditors, executive management, and the board.

Aldrich: As a GRC practitioner, I need a solid data management strategy to build a robust GRC program, so data consistency does present an ongoing challenge. I've stood up multiple GRC programs at Fortune 500 companies, and it's always an ongoing struggle. First, you need to identify what the company feels is its "source of record" for data elements. These elements can be business hierarchy, risks, key controls, IT assets, people, etc. Second, you need to determine the mapping relationships between the data. Often, you may identify the source of record but mapping relationships is difficult. In many cases, the data quality may be suspect and/or there is little agreement in business as the "true" data source for the data elements. This will always remain a big issue, but GRC platforms help consolidate the data and enforce some data consistency—even if the data quality is not 100 percent correct. It takes time for people to agree on what are these "data true sources," but you leverage what you can find and enforce the data relationships. Technology makes this issue easier but, as Marshall indicated, it's also a corporate culture issue.

Switzer: What do you think are the key success factors and leading barriers to achieving Advantaged GRC that truly supports Principled Performance?

Aldrich: The companies that are on the path to Advantaged GRC and Principled Performance definitely have common success factors. The GRC program has strong ties to the business and understands their objectives. There is an executive sponsor that supports the GRC program and an enterprise-wide scope. The GRC program is centrally managed and resourced with experienced GRC practitioners/technology implementers. Risk practitioner teams within the company communicate, collaborate, and align with a consistent risk framework. And there is an established ability to connect multiple data sources to support GRC processes/analysis.

Toburen: Foundations are critical elements necessary for the overall success of the maturity journey. Without these foundations in place, the organization will face difficulties throughout the journey either through the lack of focus, commitment, resources, or strategy. You must have:

- Management commitment to GRC culture, strategy and priorities
- Defined levels of performance and acceptable risk for GRC
- Clear expectations and success criteria defined for the GRC program
- Stakeholder support and engagement
- Sufficient commitment of budget and resources

Any organization looking to improve the maturity of its GRC program really must discuss and address these foundations. ■

{ROUNDTABLE PARTICIPANTS}

MODERATOR
Carole Switzer
Co-Founder & President, OCEG

Philip Aldrich
Director, Enterprise Risk Management (ERM) & Governance, Risk and Compliance (GRC), EMC

Marshall Toburen
GRC Strategist, Enteprise Risk Management, RSA

[GRC ILLUSTRATED]