KEY FINDINGS

RSA, the Security Division of EMC, hosted its second-annual RSA Archer® GRC Executive Forum, an invitation-only event attended by more than 50 business leaders responsible for their organizations' enterprise risk management, corporate compliance, audit, information technology, or security programs (GRC for shorthand).

GRC "integration" continued to be top-of-mind at this year's Forum. Participants typically used this phrase to mean either applying the same GRC solutions across organizational siloes or to pulling outputs of disparate solutions together, to create a unified view of risk management information. The idea of GRC integration (used interchangeably by some speakers with "harmonizing" GRC or employing a "consistent approach") referred to the process and technology aspects of GRC; it did not necessarily mean unifying all GRC activities under one director or one cross-company team.

As with 2012's inaugural Forum, GRC program owners from this year's event reported they're creating consistency in their GRC frameworks so that

RSA

information extracted from different organizational siloes share a common data structure and provide a bigger-picture view of risk and performance. “There’s no debate on the importance of integrating risk and governance silos,” said one participant. “Getting the broader view is what’s needed to promote the good and prevent the bad.”

Another theme carried over from last year’s Forum is the idea that GRC may be fading as a discrete discipline. Forum participants reported they’re continuing to drive responsibility for risk management into business units. They’re looking for ways to embed risk monitoring and controls into everyday business processes, to the point that one speaker at the event said, “Your objective should be to be invisible to the business.”

In contrast with last year’s Forum, in which GRC program managers shared strategies for winning board support, the emphasis at this year’s event shifted toward winning support for GRC initiatives from business leaders and front-line managers. This shift is consistent with the broader trend of enfolding GRC into “the business.”

Many other trends were discussed at the 2013 RSA Archer GRC Executive Forum. This document highlights recurring themes and important observations from the event.

ORGANIZATIONS FACE RAPID RATE OF REGULATORY CHANGE

In an informal audience poll (not scientific), about three-quarters of the Forum's participants said they operate within highly regulated industries. Forum participants reported that rising regulatory oversight and complexity has driven them to improve transparency across risk domains and organizational units. "It's very challenging to cope with a doubling in what we have to track with no change to process, approach or staff," said a Forum participant. Many companies are intensifying their efforts to create efficiencies in GRC policy and procedure management across different parts of the company and to improve how they map those policies and procedures to laws and regulations.

GRC researcher Michael Rasmussen shared statistics on the accelerating rate of regulatory change. In 2008, the banking industry saw 8,704 changes to key regulations; in 2012, there were 17,000+ changes. "We're dealing with increased regulatory complexity with fewer resources, so we're [pushing for a consistent GRC approach] because we can't afford not to do it," said a participant from the financial services industry.

International expansion has compounded regulatory complexity for many companies' GRC programs. "There's a crazy velocity in emerging markets to regulate," said one participant whose company is expanding its operations in China and India. "You need in-country leads where you operate whose job it is to work with legislators and regulators. That's pretty resource-intensive."

DECENTRALIZE GRC TO ADAPT TO REGULATORY CHANGE AND COMPLEXITY

To enable their organizations' GRC capabilities to accommodate the accelerating rate of regulatory change, Forum participants said they're decentralizing some GRC functions. They're distributing responsibilities such as tracking changes in regulations to regional teams. They're also driving risk monitoring to lower levels of the business.

One participant stated, "The GRC program may be owned by the chief compliance officer, but ownership really comes down to the business owners. It has helped us to have these owners documented so we know where to go when new regulatory changes come down the line and who should manage exceptions associated with the new reg. … We also have [GRC responsibilities] divided up regionally. Then, it's divided by country managers. There are people on the ground doing regional translations to identify impacts."

Another shared, "To assume we've captured all our risks is naïve. We're constantly looking for what we've missed. It has to start with relationships at the local level. Risk leaders at the local level are key to getting the data we're missing. … At first, we were surprised how many green dots we had on our dashboards and how quiet the meetings were. As trust developed, more reds and yellows popped up and communications began to flow. As trust develops among teams, a more honest picture of risk emerges because of better, more transparent data sharing."

RSA

FOCUS INTEGRATION PROGRAMS ON CONVERGENCE, NOT CONVERSION

Organizations are rationalizing multiple siloed compliance programs by mapping linkages across regulations, policies, rules, assets (such as facilities and IT infrastructure), and controls. While individual parts of the organization may have their own GRC methodologies and tools, it's up to the GRC executive owner to help harmonize approaches among groups. "GRC maturity centers on collaboration. It's up to the GRC facilitator to get people to play in the same sandbox."

A couple of Forum participants, drawing from their experiences, suggested that the most productive first step in GRC integration is to focus on converging data streams from disparate groups, not converting everyone to new processes and technologies. "We are starting at the elementary level to come to agreement [with various business] teams. We don't change how they are doing things, but bring them together into an enterprise view," said a participant who recently began a cross-enterprise GRC integration program. Another participant said, "We realized we needed to share GRC vocabulary, the taxonomy and then we can pull that through to other departments. We can't afford not to do this."

DRIVE RESPONSIBILITY FOR GRC DEEPER INTO THE BUSINESS

Expanding beyond last year's discussions on winning board- and C-level support for GRC programs, this year's Forum attendees shared strategies for enlisting active participation from business leaders and front-line managers. "You can't just have a top-down risk structure. … The more people that buy in, the better your chances to succeed."

The focus on front-line business leaders at this year's Forum did not mean GRC leaders didn't value top-level support. "Having the message top-down from senior leadership allows you to pull risk education down to all employees. You don't want to ask them to do a lot more, but make them aware. Make it easy. Get senior leaders to say, 'What does Risk think?' As soon as this is stated, you no longer have to chase people down."

Yet, beyond top-level executive support, this year's Forum attendees seemed to acknowledge that their enterprise GRC programs depended on the cooperation of lower-level business leaders. One Forum speaker observed, "You can have the best (GRC) policies but ultimately you control nothing. The business controls implementation … so you have to show how what you're doing can make their job easier and build knowledge there."

Forum participants expressed a growing sense that everyone in the company should have an ownership stake in GRC. Involving different parts of the business in GRC processes was diplomatically described by some as requiring "thoughtful planning" and by others as "painful." To enlist broader business participation in GRC initiatives, a couple of speakers said GRC program owners should focus on the process of risk and compliance assessments, not on organizational actors. "Don't let ownership get in the way, because if you get stuck on organizational change up front, you won't succeed. We looked at the process, what part [each team] had to

play, and we tried not to get wrapped around the wheel on ownership. After all, the business owner is the one who needs to be compliant."

INJECT A "SO WHAT?" INTO PROGRAM MEASUREMENTS

In an informal audience poll, just about everyone said they wanted better metrics for measuring GRC impact. In subsequent discussions, Forum participants said they do not have good ways to measure GRC success. Many felt their existing metrics focused on "project management" or process measurements. They would prefer to re-orient their program measurements on business impacts or on evidence of ethical outcomes. "What's important is that we report in 'human-speak' and what it means to the business," said a Forum participant. Another speaker at the Forum disclosed, "We force our risk owners to have 'so-what' sessions to synthesize what risk data to evaluate. This way, it's not just a simple red/yellow status indicator. We all benefit from having conversations about the risk so-whats."

For assessing ethical compliance, for which it may be difficult to develop hard metrics, several speakers encouraged GRC program owners to "avoid the 'checkbox' programs—that is, just checking the box and that makes everything okay. Think instead about the letter and spirit of law. Ethical precepts are at the base of laws. Compliance structures support ethical outcomes." Another speaker said, "In audits, the ethical response might not be the one that checks the box. You may have to ask if you're complying with the intent of the law or regulation."

TIE GRC TO ENTERPRISE PERFORMANCE

Customers with more advanced GRC programs expressed their intent to combine enterprise and operational risk management with performance management. These customers are in the process of transitioning from reporting on risk- and control-thresholds to reporting performance-focused metrics. Said one Forum participant, "Keep it as simple as possible. Collaborate with key risk stakeholders. Limit impact to the business when designing a measurement process." Many GRC program owners seem to be in the exploratory phase: experimenting with ways to tie compliance and risk metrics to business processes and business outcomes. They acknowledge their GRC programs are more mature in some processes than others, so metrics and measurement quality will differ. "Operational risk is vast. Legal is more qualitative. We have different measurements for different types of risk. Our overarching goal, however, is that we make [what's measured] meaningful to business first, not risk managers."

The push to link GRC programs to enterprise performance metrics may be driven in part by the scrutiny and support that corporate governance and risk management functions are getting from boards of directors. "We report up to the board through the board's audit committee. So, we have to match measurements to management's expectations and report at the appropriate level."

CALIBRATE CULTURE SO RISK ISN'T SEEN AS BAD

Forum participants emphasized the importance of cultivating organizational cultures that encourage openness and disclosure—even if what's being disclosed is bad news. "This a cultural shift, bringing information forward and not being penalized when you bring issues up. People often are afraid when they see [red metrics], but we have to be able to define our emerging risks in order to deal with them. Risk cannot be seen as bad." A culture of openness begins at the top. Said one Forum speaker, "If management admits issues, then the rank and file will see it's okay to do so. It takes courage to do the right thing."

ASSIMILATE THREAT MONITORING AND DETECTION INTO GRC PROGRAMS

Cyber risks have expanded, with BYOD, mobile, and cloud computing all introducing new security threats and risk management challenges. Along with external exposures, organizations must also contend with employee misbehavior. Echoing a familiar refrain often heard in the information security industry, a Forum participant said, "There are two kinds of companies: companies who have been breached and companies who know they have been breached."

GRC program owners recognize their inputs, tools, and processes must evolve with the threat. For that reason, they're exploring using a wider range of data sources and advanced analytics to make threat detection and risk assessments timelier, more comprehensive and accurate. In addition to ingesting traditional types of structured information (logs and events), GRC tools must also accommodate unstructured information, such as audit findings, social media reports, and external threat intelligence feeds.

PREPARE FOR BIG DATA IN RISK ASSESSMENTS

The data analytics methods, Big Data inputs, and data visualization tools used in other enterprise functions are now making their way into enterprise GRC programs. The use of advanced analytics tools in this domain, though, is still nascent. "It's definitely an evolution. There is overlap in the maturity elements. Take stochastic modeling … we're enamored with the results, but there's a false impression that we are going to run business by these results. It's just not there yet. We need to take a look farther into the distribution to use it for modeling." Another Forum participant noted, "Risk measurements are becoming more analytical … not just for assessments but also for forecasting." Applying big data for predictive risk analytics, not just historic analyses, will become increasingly important in the coming years.

CONTACT US

To learn more about how EMC and RSA products, services and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at www.EMC.com/rsa.