KEY FINDINGS

RSA Archer GRC Executive Forum

RSA®, the Security Division of EMC®, hosted the inaugural RSA Archer™ GRC Executive Forum, an invitation-only event attended by more than 30 business leaders responsible for their organizations' governance, risk and compliance (GRC) programs.

The Forum, held in Chicago on June 5, 2012, put the spotlight on RSA Archer customers' experiences and best practices. Participants shared perspectives from a wide variety of industries, resulting in a rich cross pollination of ideas, which are captured in this key findings document.

RSA

EMC²

BUSINESS RISKS CONTINUE TO MOUNT AND MULTIPLY.

Forum participants cited examples of the risks facing their organizations:

- Regulatory requirements continue to grow, making GRC more and more challenging. One GRC consultant at the Forum cited an extreme case in which a client designing an enterprise GRC program compiled 81,000 requirements.
- Participants expressed concerns about risks resulting from greater business complexity. GRC teams are compelled to provide enterprise-wide risk assessments, drawing on evidence from across organizational siloes. “We have to show where information comes from, how information makes its way through the organization to the board of directors,” said one Forum participant. “We have to show how the information is validated and the linkage. Without (RSA) Archer, this task would be impossible because complexity in our organization continues to grow.”
- A participant in financial services cited new business risks and security exposures arising through his firm’s use of technologies such as electronic payments, mobile banking, and cloud services.
- Participants across multiple industries said their company leaders were very sensitive to reputational risks. A chief risk officer said, “The board wants figures. They want reputational damage quantified, which is hard to do. … The front page of the paper is front and center on minds. We are keeping close track of social media, the press. A little error on our side can get magnified on Twitter. … It could blow up very quickly.”

RISK MANAGEMENT RISES TO A BOARD-LEVEL CONCERN.

Risk management is increasingly a C-level and board-level conversation. GRC program owners said they are spending more time reporting to the board about risks facing their organizations. Corporate directors are sensitive to their legal obligations for compliance oversight. Chiefly, executives and directors need to ensure their organizations’ responsibilities are fulfilled and policies observed. One participant said, “[The board is] starting to get it: regulatory pressure, news items. What really gets them is, ‘How do we know the problems being reported in other places are being taken care of here?’”

Summit participants assert that GRC processes and tools that span the enterprise is essential to corporate transparency and integrity. In the words of a speaker at the Forum, “Are you walking your talk? Or is your organization living a double life? You have to do what you commit to do. You have to be transparent. Integrity is essential to good GRC.”

To this end, corporate directors are also concerned about the accuracy and integrity of GRC information. They’re looking for reassurances that the organization is making sound risk management decisions based on reliable, representative information. A GRC program owner explained, “It’s not about putting data in front

of them; it's about putting the confidence behind it. How do they know if they can trust the information—that it's not just a self-assessment from one person way down in the weeds of the organization?" Corporate directors want to know the critical information on which they're basing risk decisions are validated by different stakeholders.

To ensure the validity of GRC-related information, Forum participants discussed initiatives aimed at expanding the number of users within their organizations (and thus the number of data points) for the RSA Archer GRC platform.

- "The purpose of the tool is not to get your risk managers to use it; it's to get your front lines to use it. We have 300 people using (RSA) Archer this month."
- "We're early in the (RSA) Archer adoption process. We used to do this in spreadsheets. Now, we can tell how many people evaluated their security controls because we can see in (RSA) Archer who did it. My visibility into the process is so much better. The tool gives us a sense of whether we have coverage in any given area. We can see what assessments have been done deep in the organization."

ALIGN GRC GOALS TO BUSINESS PRIORITIES TO WIN ADVOCATES ON THE BOARD.

Forum participants across different industries and serving different organizational functions observed that organizational leaders may be predisposed to believe that risk management functions are disconnected from business priorities. Disproving that belief and helping board members perceive business value in developing a strong GRC function is top of mind for many GRC program owners.

To help corporate leaders and directors understand GRC's contribution to business success, Forum participants offered some tips:

- "If they're a product-producing organization, you tie [the discussion] to profits. If they're a service organization, you tie it to information breach and risk. Tie it to stuff people care about."
- "We use words like 'assurance' and 'capacity' and we stopped rating risks on heat maps. Instead, we asked (corporate directors) what their risk appetite was. They set the risk appetite for us. Now, instead of a risk map, we have tolerance and capacity indicators."
- "We struggled with the term 'GRC.' For our board, it's 'operational risk management.' Using their taxonomy had a big impact. It seems like a small thing, but it helped us align the board behind our programs."
- "Keeping the board aware of the trends, what competitors are doing (in GRC), is important. We only have limited resources to do risk assessments, so I take two-thirds of them and have them handle the required risk assessments. The other one-third I focus on the board's (risk) agenda: what are the risks in expanding to foreign markets, M&A issues, etc."
- "I explain the business value of GRC this way: the fastest cars need the best brakes. GRC enables an organization to be a fast car by being the car's good brakes. GRC tells the organization to slow down on

strategy as they enter certain higher-risk areas. GRC enables organizations to be high-performing by hitting objectives in a safe and reliable manner."

GRC PROGRAMS MUST "CROSS THE CHASM" TO GET A BIG-PICTURE VIEW OF RISKS.

GRC program owners report that enterprise risk today is still largely managed in siloes. This compartmentalized view makes it hard to make enterprise-wide risk assessments. "How do we know our people are working on the right things—that we are focused on high-priority projects and what the greatest risk is?" remarked one participant. "We need to prioritize across many groups within the enterprise, not just within each silo or group."

At the Forum, many GRC program owners expressed interest in "crossing the chasm" from a siloed GRC program to a unified GRC program. An RSA Archer spokesperson pointed out that this chasm was oftentimes the "make or break" moment for enterprise GRC programs.

Program owners are pushing for uniformity and consistency in their GRC frameworks so that information extracted from different siloes will share a common structure. The goal is to facilitate a comparison of risks from different parts of the organization to help determine which risks are priorities at the enterprise level. "This enables you to build a consistent heat map across the entire organization so you're comparing apples to apples," said one GRC program owner.

Showing the delta between a unified goal state and the current state could help rationalize additional investments that may be necessary for GRC programs to grow in maturity. One GRC program owner said, "We got to a point where we needed to converge the data and look at it holistically as an enterprise. That was the chasm. We developed ORM focus areas: compliance, security, etc. We documented where we are and where we want to be. … That's what we now give to our board and executives. It is a graduated model that helps us show the gap between goal and actual states and the initiatives that we're pursuing within each."

NEW GRC DEPLOYMENTS AIM TO BUILD CROSS-ENTERPRISE VISIBILITY & INTELLIGENCE.

Some Forum participants implementing new GRC programs say their deployments have a whole-enterprise scope, rather than being confined to a particular business unit or function. These organizations recognize they can extract far greater value from GRC platforms that support a broad range of business groups and functions.

In new deployments, organizations are increasingly designing GRC roll-outs with cross-silo integration in mind. While designed to "go big," these roll-outs typically have modest beginnings: for example, an ad hoc deployment to address a specific pain point such as an audit finding or a regulatory requirement.

INVEST UP FRONT IN UNIFYING GRC PROCESSES AND FRAMEWORKS.

At the enterprise level, organizations need to decide what risks to measure and how to report on them. While this sounds deceptively simple, participants admitted that

developing a shared GRC framework for multiple groups could be very challenging. “The biggest difficulty about GRC programs is getting [the framework] right,” said one participant.

At the heart of this is understanding the board's appetite for risk so GRC program owners can set controls and prioritize activities. One GRC veteran said, “It could take two or three years to get this right.” Another said he had seen workable frameworks completed within a quarter. Timeframe aside, Forum participants agreed it is well worth investing time and resources up-front to develop shared assets such as a common risk taxonomy and a unified platform, as these streamline GRC roll-outs and ultimately help organizations realize more value from GRC programs.

In some enterprises, aligning GRC processes to business priorities requires changing how risk management functions are integrated into existing business processes. A Forum participant said, “When we first started the process, we realized it came down to the framework. The tool is secondary to the process. You’re having to change [user] behavior. It’s important to spend time up-front to get alignment.”

A participant with a sophisticated enterprise GRC program shared an anecdote of how piecemeal GRC deployments could be salvaged by planning a unified framework up-front: “We tried the top-down approach and couldn’t agree on the definition of ‘standard’ or ‘policy.’ It just didn’t work. So we rolled it out with a unified framework on the back end, but on the front end we just presented it to the groups individually. In the background, we had built the linkages and frameworks, so when people asked if they could get an integrated view with another organization we were prepared to show it. Now, the GRC reporting spans across the organization.”

Another experienced GRC program manager said, “Going back and revisiting the roadmap is very important, because things change in the organization. We update our communication strategies to our employees to market the project. It’s a simple thing, but it’s what keeps the program vital and fresh.”

Forum participants conceded that such efforts, while time intensive, proved invaluable in improving the efficacy of their programs. Participants' experiences also reinforce the need to select a flexible GRC tool that can adapt to shifting conditions.

LAUNCHING A GRC PROGRAM? START SMALL AND SHOW A HUGE IMPACT.

Forum participants said smaller-scale or even siloed deployments are not only easier to get off the ground but they’re often an effective way to prove the business case for more ambitious GRC programs. One Forum participant advised that fellow GRC program owners “Go for staggered individual victories. Take the critical risks and hit it out of the park to justify the investment. Then, each victory builds and becomes bigger. Show the step-by-step gains.”

Starting small and building up can help organizations acclimate to the changes in people, processes, and technology inherent in implementing a new GRC program. Although the test case may take months to implement, each successive roll out builds on previous implementations and requires progressively less time.

GRC program owners were quick to point out that investing in a GRC system was not just about justifying the purchase of the tool (i.e., creating a technology

business case). It's also about identifying a business need and mapping policies to controls and linking them to what people are doing. "You need to have a good, efficient, automated process before the tool."

A couple of GRC program owners suggested that organizations could find a quick win by starting with IT GRC. Because IT is well-defined, it can be used to help build an extensible taxonomy for future GRC programs for other parts of the enterprise. "If we hadn't started in IT GRC, it would have been overwhelming to build the taxonomy," said one program owner.

Another company, however, started its RSA Archer deployment from the operational side, not the IT side. This organization wanted to remove 50,000 hours from its audit process, which was managed in Excel spreadsheets. Then, the organization rolled out the GRC program to 1,200 locations in the U.S. and Canada. As a result, "Every audit in fiscal year 2012 was an exceptional audit opinion. The tool works. The process works. There are ways to tie in the value. … We eliminated [audits amounting to the work of 12 auditors per year]. The number of audits that we won't have to do because of (RSA) Archer can justify the investment."

PROGRAM OWNERS WANT TO ACCOUNT FOR "SOFT COSTS" IN MEASURING GRC BENEFITS.

GRC program owners said they were under pressure to demonstrate to corporate executives and directors a strong ROI for their GRC programs.

Forum participants observed that much of the value captured by using the RSA Archer platform was difficult to quantify. "[RSA Archer is] a hard-dollar cost, but it's a soft-dollar return. … We have a consolidated implementation team. If I ask for an FTE, I get 0.2 here, 0.3 there. With a distributed model, it can be hard to [track and take credit for] all the returns. You don't see that you saved three FTEs somewhere else. The costs are consolidated but the benefits are shared. We've begun to analyze our impact so we can begin to talk about savings in other places, even though it may not 'belong' to us."

Another Forum participant provided a concise summary: "While the (Total Economic Impact research study from Forrester) is nice, what we're looking for is an efficacy assessment. The investment in a GRC system can be a rounding error (to corporate executives). What they're interested in is the process impact."

"When you provide information at the board level on (a risk management) process, I find it helpful to communicate findings and their potential impact. Articulate the degree of uncertainty. Provide an analysis that shows a disparate degree of uncertainty and how, with more funding, we can narrow that uncertainty. And then let [the board] set the level of acceptable uncertainty. Ask them what their risk appetite is and map to that."

WILL GRC FADE INTO THE SUNSET AS A DISCRETE DISCIPLINE?

Many Forum participants affirmed that GRC as a discrete discipline is fading within their organizations. Instead, participants reported they're increasingly integrating GRC processes into enterprise/operational/information risk management programs. Forum participants referred to these programs by various names, including ERM, information risk management, and operations/operational risk management.

One Forum participant said, “GRC as a standalone process is becoming obsolete.” GRC is folding into broader programs to manage risk across the enterprise.

Another participant said, “True success for us is that GRC goes away. The long-term strategy is excellent process management, and GRC is just the underpinnings of that.”

GRC PROGRAM OWNERS SEEK TO LEARN FROM EACH OTHER.

Forum participants’ GRC programs represented a wide range of maturity, both in terms of GRC platform adoption and organizational sophistication in managing GRC programs. Similarly, participants in the Forum represented a wide range of job titles, from chief risk officers to IT program managers. In the post-event survey for the Forum, most GRC program owners wrote that they saw high value in interacting with their peers and in learning what other companies—especially those in other industries—were doing in risk management. GRC leaders also expressed interest in sharing best practices to build the discipline of risk management.

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.