AMR Research Alert Article

The Governance, Risk Management, and Compliance (GRC) Landscape, Part 1: A Segmented Marketplace With Distinct Buyers

Monday, June 23, 2008

John Hagerty, Dennis Gaughan

During the early days of governance, risk management, and compliance (GRC) software, fueled largely by the Sarbanes-Oxley Act (SOX) requirements and a slavish attention to compliance, AMR Research predicted broader platforms would eventually emerge that addressed multiple compliance initiatives in a consistent, cogent manner. To a large extent, that process has begun. More than a handful of vendors have assembled GRC-based platforms through organic expansion, acquisition, and partnerships to address multiple GRC concerns.

As risk management activities accelerate (it's now the primary motivator for GRC-based investment), defending against operational, IT, brand, reputation, regulatory, and financial exposure is a top priority. These grander issues might be expected to lead to all-encompassing technology purchases and standardization on a common platform.

Although seeing some value in a unified approach, buyers still evaluate and purchase products and services based on specific initiatives. This dynamic has led to a splintering effect, with business-led GRC and IT-led GRC programs each having their own sponsors and budgets. While there is surely some overlap, they are largely evaluated separately.

GRC demands a consistent taxonomy to define specific market segments and buyers

AMR Research has always taken an expansive view of governance, risk management, and compliance to identify, organize, manage, execute, and enforce policy and procedure. With that in mind, we have developed a taxonomy that will be used to evaluate vendor position in the various segments of GRC (see Table 1).

Table 1: GRC Taxonomy

GRC Management *Manage risk and compliance programs within and across the business*	Definition
Risk & control framework	These are applications that define, manage, monitor, and display the varied GRC programs any company manages.
Risk management software	These are products that allow companies to identify, assess, categorize and prioritize risks at the enterprise or operational levels of the business.
Dashboarding and reporting	Tools and/or applications that enable businesses to track key performance and risk indicators by providing a unified view of GRC status and performance on an integrated, timed, or near-real-time basis.
Inititive-specific content	Different risk/compliance initiatives may have pre-defined models available to accelerate management of that initiative (e.g. Sarbanes-Oxley risks and controls, IT governance frameworks, 21 CFR Part 11 for Life Sciences, etc.)
GRC Execution *Monitor and take action on risk and compliance issues defined within GRC Management*	Definition
Access controls products	Products that automate checking of controls and/or compliance rules and actively identify which users/roles have access to what functions and manage any violations of span of control, as defined by company and/or best practice.
Identity management products	Ability to centrally manage the provisioning and de-provisioning of identities, and to consolidate the proliferation of identity stores.
Business process controls products	Products that automate checking of controls and/or compliance rules for any business process to ensure activity is conducted according to policy, procedure, and/or prescribed process as defined by company, best practice or regulation.
Audit testing tools and applications	Independent tools and products that allow internal and/or external advisors to validate business transactions and identify fraudulent activities or fractured business processes.
Data security products	Products that discover, classify and enforce controls on sensitive content residing in structured and unstructured forms, including personally identifiable information, financial records or intellectual property.
GRC Application *Purpose-built applications to manage industry and process specific risk and compliance issues*	Definition
	Myriad products (for example: environmental health and safety (EH&S), global trade management, corporate social responsibility, supply chain and other operational risk, or IT risk management, etc.) that manage specific isssues

Download Larger Version

Source: AMR Research, 2008

We've wrestled with this categorization issue for a while:

- Is GRC all-encompassing, including any governance, risk management, and compliance concern across the extended enterprise?
- Is GRC only IT and administrative concerns?
- Is operational risk and compliance part of the definition?
- Is GRC an organizing theme and not a distinct technology market category?

We definitely consider GRC a set of processes with supporting technology products. But it is segmented into specific classes of product (as defined in the taxonomy), with its components appealing to different buyers in the organization.

Without some type of organizational qualifier (business led, operational, or IT) or category name (management, execution, or application), GRC is only an organizing theme for separate but related activities.

Buyers recognize GRC holistically, but continue to buy at discrete pain points

Discussions with clients, either individually or in group settings, led us to some blatant conclusions:

- Companies recognize GRC as an important theme, with policy, procedure, and related software and service components.
- They have a hard time understanding the connections between what they see as disconnected functions conveniently grouped by vendors under the GRC moniker.
- They purchase individual components to manage specific needs as identified by business and IT users.
- While buying may include more than one module, it's not a suite that's being purchased.
- Firms distinguish between transaction-based requirements versus management-based necessities.

A tactical approach still predominates

Companies report they administer risk and compliance concerns in isolation. Managers are responsible for different pieces of the puzzle, with limited cross-organizational oversight and coordination. While this is today's reality for many, they do voice a need for consistency and visibility across the silos, but the impetus to do

something about it remains relatively weak.

GRC has not matured to the point where the majority evaluates and purchases a broad suite of related capabilities. To put this in a historic perspective, think back to the emergence of ERP:

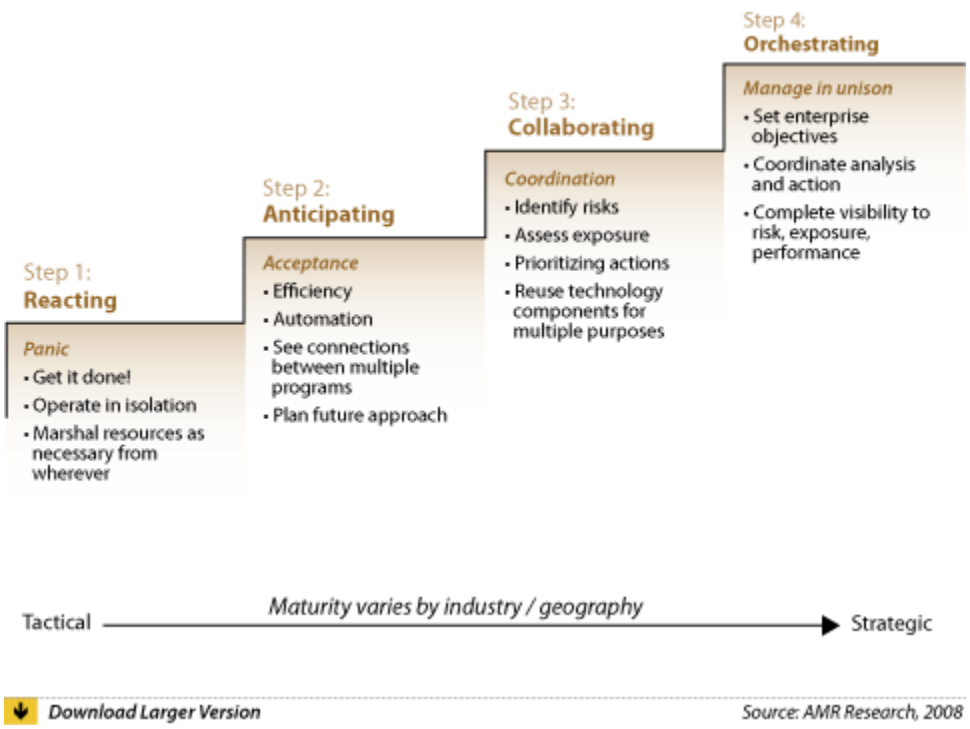
- In the 1980s, the components of core ERP—general ledger, accounts payable, accounts receivable, fixed assets, human resources (HR), and payroll—were evaluated and purchased separately. It wasn't uncommon to find a mixed bag of products from different providers that didn't recognize the other existed.
- In the early 1990s, these products were clumped in larger groupings: core financials or human capital management (HCM).
- By the late 1990s, these products were largely purchased and implemented as part of an integrated suite from one vendor.

GRC is following a similar maturity path. In 2008, we see GRC now where ERP was in the late 1980s: not with solely independent functions, but ones that are starting to cluster together based on a common set of buyers. The two major buying centers we see are IT (the CIO's office) and business (CFO, operations, and risk). Within the business segment, there are many potential buyers, depending on distinct business drivers.

Risk management is the new compliance

One benefit of having a long history with GRC is that we've seen companies go through a fairly typical set of phases. AMR Research's GRC maturity model was developed in late 2006 and holds as true today as it did when we first introduced it (For a detailed discussion of this model, see "From Tactical to Strategic to Holistic: AMR Research's GRC Maturity Model").

Figure 1: AMR Research's governance, risk, and compliance (GRC) maturity model



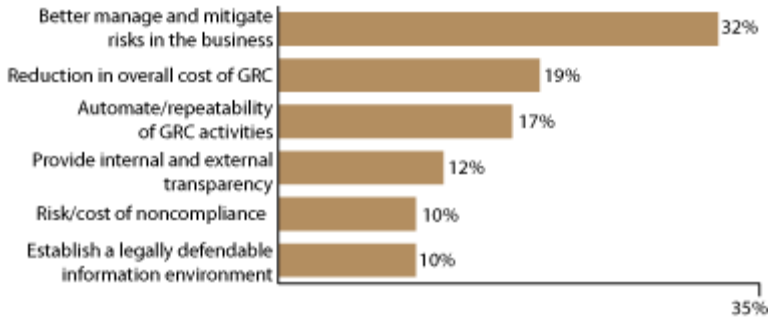
Download Larger Version

Source: AMR Research, 2008

Risk thinking is maturing

Starting in 2007, we noted that risk jumped significantly in importance as a key GRC motivator. In 2008, it is now the No. 1 influencer by a wide margin, followed by cost reduction and automation of GRC activities (see Figure 2). Compliance used to be the central theme that originally drove GRC awareness. Compliance, as well as risk of noncompliance, was also the primary driving force behind technology and service investment.

Figure 2: Most influential issue driving investment in GRC



Download Larger Version

Source: AMR Research, 2008

How do you assess risk? After all, one company's risk may be another's opportunity. Tolerance for risk will differ—in many cases, significantly—by individual. Organizations are now willing to engage in internal debates on risk, keen to understand how to frame the issue within organizational silos and across the enterprise. For now, they are looking for advisors to help them work through the process.

Seeing the forests versus the trees

Many business and IT executives candidly report they are not sure how or when to act on what they uncover (or even if they should), but they are open to systemically identifying, assessing, prioritizing, and mitigating the right risks across the business.

In 2008, risk equals or exceeds financial governance concerns across all discrete buyer groups. For this reason, we can comfortably declare risk management is the new compliance. It dominates many GRC interactions, with buyers animated when explaining how they can and will make risk-aware decisions that concretely affect overall business performance. For customers, compliance regimens provide a crystal-clear view of the trees, with risk management allowing them to see the forest.

IT risk is clearly a separate buying center

All parts of the business are now focusing on better risk management. While this shift is largely driven from the top down, it has quickly taken hold in IT organizations, since much of this stems from the significant role IT plays in supporting myriad compliance requirements.

The inability to assess risk has also been flagged as a critical gap for many of AMR Research's clients. In fact, customers that have taken our IT assessment based on the COBIT framework often have "assess risks" as one of their biggest control gaps.

IT risk management, a component of operational risk, is an emerging focus area for companies that recognize the effect IT can have on their overall risk management strategies. It has clearly emerged as a distinct GRC audience, with its own concerns and budget (see "IT Risk Management Spending Report, 2008–2009: Elevating IT Risk as a Critical Component of GRC" for more on this).

GRC management programs will eventually be linked with pervasive performance management

At the highest levels of GRC maturity, the firm operates and manages in unison. Strategies are clearly articulated and mapped directly to operating models. Enterprise-level risk management is done formally, with all manner of risk identified, categorized, assessed, and prioritized.

Rather than having each group doing its own thing, the company has a clear, defined protocol for managing a risk portfolio. When stacked next to other priorities, one group's hot risk exposure may pale in comparison to others. Companies make the tough call of the risks to address and the ones to accept. The connection to pervasive performance management (PM) is strong, with visibility into key performance and risk indicators fused into one cohesive management system.

Today, GRC and pervasive PM are run and managed as separate programs, but the attributes of companies operating at peak level in each area are strikingly similar. AMR Research believes the management aspects of GRC will eventually fuse with pervasive PM initiatives.

Conclusions

The market for GRC is segmented into three major areas:

- **GRC management software**—To organize risk and compliance programs across the business
- **GRC execution capabilities**—To monitor and take action on risk and compliance issues defined in GRC management

- **GRC applications**—To address specific business processes as identified by regulatory agencies across the globe or industry-led consortia

Companies evaluating software and services for governance, risk management, and compliance should have a clear picture of what they are trying to accomplish and what their midterm to long-term goals are before they choose providers to look at more closely.

While today's buyer is largely concerned with tactical issues, others are taking a broader, holistic approach to GRC as they forge the link to broader pervasive PM programs.

Whether the buyer is the CFO, CIO, COO, or a risk and compliance office, breadth and scope are the essential first steps to tackling any GRC program.

Coming next

In Part 2, we will categorize a plethora of vendors against AMR Research's GRC taxonomy in order to advise companies on the vendors that deliver specific capabilities and products.

We look forward to your feedback and ideas—jhagerty@amrresearch.com and dgaughan@amrresearch.com.