

Identifying GRC Projects with an ROI for Organizations Using Oracle Applications

I recently read an article in CFO Magazine titled “GRC: The Solution Remains Elusive” (January/February Edition – see full article at: <http://www.cfo.com/article.cfm/14470743>). This article makes some great points and reminded me that the GRC market is still confusing for many. The article calls the GRC software market a ‘mess’ and indicates that “customers increasingly find that their ‘jury-rigged’ solutions aren’t up to the task.”

Managers responsible for implementing GRC within their organization are often still overwhelmed with what “GRC” means and how to identify and evaluate vendors who match their organization’s objectives. If you are a buyer in the Oracle applications space you may hear names such as Absolute Technologies, Approva, Archer Technologies, BWISE, CaoSys, Greenlight Technologies, Guardium, HP, Integrity, Lumigent, MetricStream, Mentissoftware, Open Pages, Oracle, QSoftware, Quest, Paisley, Ringmaster, SAP, and Tripwire. Within the Oracle suite of products you may hear solutions such as GRC Manager, GRC Controls, GRC Intelligence, Internal Controls Manager, Identity Manager, Data Masking Pack, Audit Vault, Database Vault, and Transparent Data Encryption. Some of the Oracle solutions are technology solutions that may or may not be supported by the application(s) your organization uses or the specific version of the application(s) you use.

Many are still confused by the question highlighted in this article, “what is the GRC market?” Since the definition of GRC is still unclear, it can mean many different things to many people. Anyone with software that helps with monitoring and automation of internal controls can (somewhat...) rightly claim they have software in the ‘GRC’ space. So... you have a wide variety of companies with varying applications competing for budgets and mind-share of the C-level executives. Perhaps one day the definition of GRC will become clearer or ‘sub-definitions’ will emerge. As I look at the landscape, I see two distinctive types of applications – business-oriented and those that are IT-oriented.

Business-oriented software generally focuses on these activities:

- Assistance for the corporate board and C-Level executives in managing their organization’s overall compliance efforts
- Documentation of controls and the attestation / audit management process
- Identification and administration of risks and corporate governance
- Compliance with laws and regulations

IT-oriented software generally focuses on these activities:

- Monitoring of controls within IT systems such as ERP systems and legacy application – at various levels: OS, database, and application – often referred to as Continuous Controls Monitoring or Continuous Auditing
- Automation of controls such as segregation of duties, data security, change management, and intra-form conflicts

Admittedly, our practice focus has been more on IT-oriented applications and applying the ‘theory’ of risk management (i.e. identification and mitigation of risk) to IT systems and related ‘GRC’ software. So,



we'll focus the rest of the article primarily on IT-oriented applications and those primarily at the database and application levels.

Obtaining an intimate understanding of the technologies and processes of each of these applications is necessary to ensure that you don't buy a 'pig in a poke.' Because of the diversity of features and technologies being sold by these software providers and varying objectives for each organization, there is no easy method to obtaining this understanding. Therefore, it is advisable to use a reputable firm such as ERP Risk Advisors, Corporate Integrity or a myriad of other firms to help navigate through this labyrinth.

Many advantages can be attained through the use of "GRC" software packages. These include: reduction of risks, compliance with laws and regulations, reduction in external audit fees, reduction in internal costs for documenting and testing controls, and detection/prevention of fraud. Some of these benefits result in 'soft' cost savings or avoidance and some result in tangible 'concrete' savings and both angles are necessary and dependent on management to prioritize. However, in today's tough economic times C-level executives are often taking a 'show me the money' (i.e. savings) approach to GRC projects.

The article quotes Ventana Research analyst Robert Kugel as saying "There's no arguing that from a buyer's perspective, 'GRC software' doesn't exist today.'" This comment seems rooted in the frustration that there is not a one stop comprehensive solution to meet an organization's GRC requirements. There are maturing solutions in both the 'business-oriented' and 'IT-oriented' solutions. If the comment is implying that there is no single source vendor offering a mature solution, I'd agree (albeit my understanding is more related to Oracle's applications).

I'd argue that a single source vendor who thoroughly covered both the business and IT applications is a pipe dream. To build this 'Cadillac' of an application, you'd need a thorough understand of risk management on one end of the spectrum and a very detailed knowledge of particular applications (such as SAP and Oracle) and their related technologies on the other end of the spectrum. In between, you'd need comprehension of controls design and the audit management process (testing, remediation, certifications, CCM, etc.).

Oracle's GRC applications are a perfect example of this. Their GRC Manager tool addresses the risk management and compliance elements and their GRC Controls tools address the CCM and controls automation elements. However, much to the chagrin of buyers, there is little integration between the two suites.

If there is to be a mature convergence of both the business and IT applications, it will likely take place within the large ERP vendors – Oracle and SAP. Oracle and SAP have both been aggressive in acquiring smaller niche players to complement or supplement their existing offerings. I'd also argue that this convergence is likely to be slow and incomplete leaving room for various niche players to fill gaps left behind by the 'big boys.'

One point we definitely agree with in the article is the comment that "Before risks can be managed, they must be identified." Rather than hypothesizing about what risks need to be managed, we'll give you a list of risks that your organization may still need to address. To the C-level executives that are tasked with addressing your organization's GRC Objectives, I'd say START WITH WHAT YOU KNOW... and START

WITH WHAT SOFTWARE IS AVAILABLE on the market. Instead of seeking out something that doesn't exist, a savvy GRC buyer should start with understanding what solutions are on the market and then determining if the cost/benefit analysis leads to a reasonable and acceptable ROI.

Here is a list of the common issues we've seen organizations still need to address:

- Proper application security design, including SOD issues as well as single function risks that address both compliance issues (such as Sarbanes-Oxley) and sub-material fraud risk
- Comprehensive test process for patches, often the result of poor impact analysis, for both process changes as well as application security changes
- Development of a strategy to secure and/or scramble sensitive data, in both production and non-production environments; for both access through the application as well as through direct database connections
- Comprehensive peer review process for new development including impact of access to sensitive data
- Comprehensive change management process that takes into consideration changes being made through objects and security configurations, as well as application configurations through the forms
- Development of comprehensive audit trail using a trigger or log-based solution to build before/after values to support a myriad of objectives including controls related to fraud, operational stability of the system, consistency in process design, and an audit of the change management process
- Intra-form issues resulting from multiple constituents needing access to a single form (deficiency in the design of the forms/functions)
- Ability to continuously monitor controls and provide proactive notification when certain conditions are met
- Extraordinary access by business analysts and other personnel (aka privileged users)
- Monitoring of activity through forms that allow SQL statements (and OS scripts) to be executed within them
- Failure to harden apps tier and database tiers appropriately, including re-reviewing such requirements after patches are applied

From our experience, solid reasonably priced software solutions exist that address the majority of the issues. These offer the following:

- Continuous controls monitoring / Continuous auditing
- Segregation of duties and user access controls analysis, including optional features such as preventive controls, SaaS offerings
- Data security – both in production and non-production environments; at the application level as well as the database level
- Data scrambling in non-production environments
- Preventive controls where the application's security design or application's process design is not sufficient to support defined controls
- Building a detailed audit trail (before/after values) using trigger or log-based technologies to support audit requirements for fraud, application controls, implementation reviews, change management best practices (security, development, configuration, and patching)
- Comparison of information between instances and between points in time



- Monitor the apps tier and database tier hardening requirements, including re-reviewing such requirements after patches are applied
- Manage risks across platforms with adapters to connect to various ERP systems as well as legacy systems

While other firms have narrowly focused on compliance initiatives such as Sarbanes-Oxley, we've been focusing our efforts on identifying best practices and working to identify software solutions with appropriate content and technologies to address your organization's control objectives. If you focus on known issues and resolve to fill the gaps, when new compliance initiatives come, you'll have the appropriate technology (ies) in place to address them.

To find software providers with a rapid ROI, look for some of these features:

- utilizes an architecture that allows it to be extended to other requirements in the organizations
- offers automation capabilities along with monitoring of controls that cannot be automated or are cost prohibitive to automate
- provides as much embedded risk-based content and best practices as possible

Remember that most software companies rely on consulting firms to help sell their solutions to their customer base. Don't expect large software providers to 'complete' their suite with all the content your organization needs as this takes away from their consulting partner's ability to build service engagements around their offering.

Further, you need to be aware of the pros/cons of dealing with smaller niche providers versus large providers including how the technology integrates with other applications and your overall IT portfolio. A CIO, in conjunction with other C-level executives and the board needs to have an overall comprehensive strategy.

Do your homework and choose wisely...