

Finance and Audit GRC Software Market Is Expanding

Tom Eid, French Caldwell

Organizations are expanding investments in software to support corporate governance, risk management and compliance. Total software revenue for this emerging market is forecast to grow approximately 24% annually through 2010.

TABLE OF CONTENTS

Strategic Planning Assumptions.....	3
Analysis	3
1.0 Forecast Overview.....	3
2.0 GRC Vendor Taxonomy and Forecast.....	4
2.1 Software Vendor Taxonomy.....	4
2.2 Finance and Audit GRC Forecast	5
3.0 Market Drivers and Inhibitors.....	6
3.1 Market Drivers	6
3.2 Market Inhibitors	7
4.0 Key Findings.....	7
5.0 Recommendations.....	8
5.1 Recommendations for Software and IT Services Providers.....	8
5.2 Recommendations for Business Users and IT Organizations.....	8
Recommended Reading.....	9

LIST OF TABLES

Table 1. Vendors Providing GRC Software Products.....	4
Table 2. GRC Software Forecast, Worldwide Total Software Revenue, 2005-2010 (Millions of Dollars)	6

STRATEGIC PLANNING ASSUMPTIONS

By 2008, more than 75% of large and midsize companies will purchase new compliance management, monitoring and automation solutions (0.8 probability).

Through 2012, fewer than 30% of companies will pursue an integrated strategy of a risk-oriented approach to compliance, standardization of controls and automation, thereby limiting the value of compliance investments (0.7 probability).

By 2012, the number of regulations that directly affect IT operations will double (0.7 probability).

ANALYSIS

1.0 Forecast Overview

Compliance regulations worldwide are driving the high-profile business and IT activities of financial compliance, corporate governance and risk management. The requirements and market opportunity are worldwide in scope because companies that are U.S. Securities and Exchange Commission registrants must comply with the Sarbanes-Oxley Act of 2002 (SOX), regardless of where their headquarters are located. In response, some countries, such as Canada and Japan, have aligned their own financial reporting rules with SOX.

In May 2006, the European Union promulgated a new company's law directive that requires its members to enact internal controls and audit independence regulations that, with the additional requirements to establish risk management programs, could be perceived to go further than SOX in new demands for corporate governance improvements and transparency.

Many organizations are now establishing an overarching governance, risk and compliance (GRC) life cycle program that consists of the key elements of identifying, planning, implementing, monitoring, analyzing and remediation. Most regulations are aimed at processes, governance and reporting and contain five steps that are aligned to the compliance life cycle:

- Step 1: Know who wants you to do things — Identify the appropriate regulations that apply to your organization.
- Step 2: Know what to do — Interpret the regulation for the organization's environment.
- Step 3: Know what you do — Understand and document the organization's processes and policies.
- Step 4: Do what you say — Monitor for compliance and changes.
- Step 5: Say what you know — Report as required.

The goals of Step 2 and Step 3 are to bring processes into compliance. The IT organization should look at these steps as they apply to the IT management processes:

- Operations — Users, third parties and functional activities
- Risks and controls — Assess, monitor and control thresholds and functions
- Reliability — Problems, incidents and security
- Records and data — IT architecture and data management

- Systems — Configurations and procedures
- Change — Quality, change management and accredited systems

GRC solutions address these six processes by integrating technology into technical and nontechnical business processes to better-document them and, when needed, change them. A key element of GRC is the ability to document and effectively communicate, informally and as a matter of record, about compliance-related issues.

Compliance represents the means of meeting the requirements of governance. Corporate governance is the framework for how decisions are made and provides the policies, laws and standards for an organization's governance framework. Operational risk management as applied to IT ensures system and process integrity, security and business continuity.

2.0 GRC Vendor Taxonomy and Forecast

2.1 Software Vendor Taxonomy

"Governance," "risk" and "compliance" are general terms that can apply to a wide range of products, IT initiatives and business requirements. Gartner, as aligned to both a supply- and demand-based market perspective, has developed a specific market structure for these general terms, as *governance, risk and compliance* (or GRC).

As used in this report, GRC is a selective focus that concerns the use of content management, compliance reporting, workflow and controls automation technologies, among other software products, to be used in support of audit, financial management, operational risk management (including compliance risks) and reporting processes. GRC requirements are determined by regulations such as SOX in the U.S. and related regulations in other countries, or by other nonregulatory compliance that may emerge from binding requirements with business partners or through corporate policy.

Software offerings in the GRC market support the compliance management process, audit management and analysis, controls automation and monitoring, operational risk management, and legal discovery. The GRC market is further segmented into these categories:

- Finance and audit GRC
- IT GRC
- Enterprise risk management
- Industry-specific GRC
- Other forms of GRC

This report focuses on finance and audit GRC, which includes finance management GRC, audit management, audit data extraction and analysis, segregation of duties, and business rule management software. Table 1 shows a representative alphabetical listing of vendors providing related software products.

Table 1. Vendors Providing GRC Software Products

	Business View	Representative Vendors
Finance Management GRC	Management, workflow, documentation and reporting associated with financial controls	Axentis, Certus, IBM, Movaris, OpenPages, Oracle, Paisley Consulting, Qumas, SAP

	Business View	Representative Vendors
Audit Management	Internal audit work papers, task management and workflow	PricewaterhouseCoopers, Paisley Consulting
Audit Data Extraction and Analysis	Tools for extracting data from business applications and running ad hoc analysis or templated queries	ACL, IDEA (CaseWare)
Segregation of Duties	Ensuring that personnel do not have access to data in a way that creates the potential for fraud	Approva, Oversight Systems, Virsa Systems (SAP)
Business Rule Management	Monitoring transactional data in accordance with business rules established as controls	170 Systems, Infogix, webMethods

Source: Gartner (November 2006)

Software products for continuous automation and monitoring are included in the categories of segregation of duties, audit data extraction and analysis, and business rule management. While these products focus on those functions and activities in which the IT organization is enforcing controls for others, their true benefit is to the finance organization through providing process improvements and transaction monitoring.

While not part of the GRC functionality set, other software technologies have benefited from a compliance label. Technologies and related markets include application integration and middleware, configuration and change management, enterprise content management and records management, HR management, IT operations management, policy enforcement, and security (user setup, identity and access management, and event management).

For example, Gartner acknowledges, and clients must understand, that many technologies are purchased in the name of compliance that may not necessarily be GRC products, resulting in blurring the boundaries that define the GRC market. This is particularly true of traditional security products that may be required as the result of a compliance audit but are not, in and of themselves, compliance products. For example, several organizations have chosen to invest in security event and information management (SEIM) products to address compliance requirements, but Gartner does not consider the SEIM market to be part of the GRC market.

Gartner clients may seek more clarity through their motivation for purchase, the buying center and which budget is used. However, this differs significantly from organization to organization and may not match Gartner's description of the GRC market or any vendor's positioning of its product. For more information, see "Sarbanes-Oxley Spending Continues to Disrupt Software Purchases."

2.2 Finance and Audit GRC Forecast

Four years after the passage of SOX, organizations are implementing more-structured responses, and vendors are providing more-comprehensive offerings. What was initially treated as an initial tactical project is evolving into a more-comprehensive process approach, expanding beyond SOX-based remediation, in support of other country-specific (Canada Bill 198, Euro-SOX and Japan's J-SOX) and/or vertical market regulations (such as Office of Management and Budget Circular A-123 for U.S. federal government agencies).

This forecast updates the new license revenue forecast in "Financial Compliance Process Management Offerings Emerge to Support Corporate Governance" and includes revenue for finance and audit governance, risk, and compliance software (see Table 2).

Table 2. GRC Software Forecast, Worldwide Total Software Revenue, 2005-2010 (Millions of Dollars)

	2005	2006	2007	2008	2009	2010	CAGR (%) 2005-2010
Total Software Spending	293.8	389.8	491.1	604.0	724.7	855.2	23.8
Note: Gartner defines total software revenue as revenue generated from new licenses, updates, upgrades, subscriptions and hosting, technical support, and maintenance. Revenue from professional services, training and certification, and hardware is not included in total software revenue.							

Source: Gartner (November 2006)

3.0 Market Drivers and Inhibitors

Since 2002, most spending on compliance projects has focused on professional services' strategy consulting, audits, process management and workflow, documentation, and planning. Funding is now shifting from services to software as organizations have completed their first phase of compliance efforts and are evaluating responses to compliance regulations. There is also a shift from a content focus to a data focus for compliance and risk management. As such, more emphasis is being placed on transactional systems, monitoring, visual reporting through dashboards and real-time analytics.

Compliance efforts are not an IT problem; organizations must realize that the combined efforts of executive teams, business managers and IT personnel must be brought together to address issues holistically.

3.1 Market Drivers

Many factors affect the growth of the GRC market:

- Phased approach to compliance support — A shift is occurring from tactical and reactive to more-strategic and proactively coordinated implementations; strategic planning will drive heightened spending for new compliance, risk management and corporate performance management solutions.
- More public and private organizations will deploy functionality — More organizations will implement GRC solutions. Midsize, government and nonprofit organizations are looking for GRC-based offerings.
- Broader regional adoption — A push is taking place outside of the U.S. to follow the SOX requirements. Canadian and Japanese regulators have adopted new rules that are similar to U.S. rules for internal controls on financial reporting. In Europe, because of competitiveness for investment and a trend toward demonstrating and proving corporate responsibility, new regulations are on the way, including requirements for risk management and having external auditors report on internal controls. Other developments in audit and regulations, such as International Financial Reporting Standards and Basel II (for banks), are encouraging companies worldwide to improve financial processes, which then leads to an emphasis on improving internal controls. As the European Union Data Protection Directive set a standard for privacy regulation, SOX is setting a standard for corporate governance regulation.
- More-robust and more-integrated offerings — Vendors will deliver better-performing, more-integrated and more-comprehensive products. Some GRC vendors already incorporate limited continuous automation and monitoring functionality, and many others have it planned for future versions.

3.2 Market Inhibitors

Market factors can also inhibit the growth of the GRC market, including:

- Concern and confusion regarding vendors and their technologies and control requirements and options — Gartner has identified more than 50 vendors that can provide some type of GRC and continuous compliance offering; however, consistent functionality does not exist across the vendors. Organizations are confused about the level of controls that must be put in place.
- Strong regional vendor presence only in the U.S. — Most vendors that provide some type of GRC offering are based in the U.S., and those that aren't focus their sales efforts on the U.S. It will take time for non-U.S.-based vendors to establish market presence in other regions.
- Market consolidation — Mergers and consolidations of large (PeopleSoft-Oracle) and small (eOnehundred Group-Stellent) companies are beginning to create uncertainty about vendor selection and product offerings.
- Availability of IT budgets and IT priorities — IT budgets have been constrained, and remedial efforts still must be completed before organizations can gain the full benefits of a GRC solution.

4.0 Key Findings

Most companies are still organizationally, functionally and technically disaggregated, which can impede business success and make it harder to comply with governmental regulations. As organizations begin to take a more-holistic approach to GRC management, there will be stronger linkages between compliance initiatives, risk management and corporate business strategy, which should, in turn, develop better alignment of people, processes and technologies. However, there will not be a single buyer or buying center for GRC offerings for some time because of the fragmented use of too many technologies that have been purchased, deployed and managed separately, as well as because of a similarly fragmented IT and line-of-business management structure.

Many software vendors have jumped onto the SOX and compliance "bandwagon," touting comprehensive solutions and even SOX-branded products. However, no single SOX risk management or corporate governance software market exists. A GRC market is emerging that focuses on the key functions of decision support and status reporting for managers and executives who are accountable for compliance, internal controls documentation and testing, workflow for reviews, approvals and collaboration, and reporting to support the audit function.

Regional adoption will slowly expand as other countries implement new compliance regulations. Many GRC implementations are in the U.S., primarily because of stringent federal penalties. Other countries, while developing compliance regulations, have yet to include the same type of punitive effects. Although growth will occur from non-U.S. companies that trade stocks on American stock exchanges, broader regional adoption will take many years. However, much of the future growth will probably come from Japan (where new regulations are appearing in 2006) and Europe (where SOX-like regulations will be rolled out during the next several years).

Software markets usually follow a fairly consistent cycle and series of phases: from embryonic to emerging, high growth, consolidation and maturity, and then decline. The GRC market is in the emerging phase and is about to make a transition to the high-growth phase. Vendor consolidation will coincide with new vendor entrances, and an additional technology convergence is expected as best-of-breed offerings compete with evolving suites and platform offerings. Many vendors

indicate that the average deal size has actually increased since 2004; this is one indication that initial deployments are expanding to larger user bases.

5.0 Recommendations

As software technologies and markets mature, a broadening and overlap of functionality occurs that was once delivered as a point offering. For larger software vendors or vendors with a market leadership position, single products develop into a platform that includes multiple applications and functions. Although best of breed is still available from smaller or niche-functionality vendors, a natural tendency exists for larger vendors to promote suites and integrated platforms over point products.

5.1 Recommendations for Software and IT Services Providers

For software vendors that want to enter or participate in the finance and audit GRC market:

- Determine the best fit of your offerings within the broader compliance environment; a "one size fits all" approach does not exist, and offerings must be tailored in appropriate ways, such as for finance and audit GRC or continuous automation and monitoring.
- Implement a well-integrated suite of products with seamless navigation and information, and context transfer between internal components and external applications. Document and records management, collaboration, decision support, and other technologies must be tightly connected with common interfaces to financial applications and application "adapters" and "connectors" that can act in real time.
- Evaluate options for OEMs and partnering to fill functionality gaps. Seek partnerships and software components that will complete client requirements for continuous automation and monitoring management. Focus on configuration management, change management and segregation-of-duties capabilities.
- Establish subject matter expertise regarding use cases, best practices and thought leadership within your services organization and through your software.
- Examine partnerships with systems integrators for implementation expertise.
- Many organizations have varied technology deployments and limited process integration. Identify the uses and intersections of technology, process and business function, and align your offerings accordingly. Provide templates and pre-defined process flows for faster process automation.

5.2 Recommendations for Business Users and IT Organizations

If you are a business user or a member of an IT organization:

- Regard any stand-alone or SOX-specific solution with skepticism. Extensibility to other regulations and to general risk management is a benefit.
- Address regulations systematically to enable business units to build on their collective experience, processes and technologies. Companies that adopt these practices at a high level and instill them in their corporate culture will have an easier time abiding by SOX requirements and other forms of compliance regulations.
- Work with auditors to identify compliance issues and then fix those issues, instead of buying a software tool to do the auditor's job.

- Automate the execution of repetitious control functions, and focus on aggregating common control features that leverage your financial control framework.
- Implement a strategic, phased approach because more investments are required to deploy new solutions and retrofit established systems.

RECOMMENDED READING

"Survey on Sarbanes-Oxley Compliance Practices Within IT Organizations and Businesses"

"Childhood Ends: Liability and the IT Industry"

"Sarbanes-Oxley Spending Continues to Disrupt Software Purchases"

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509