Gartner Dataquest

Publication Date: 19 December 2007 ID Number: G00153270

Dataquest Insight: The Finance and Audit GRC Software Markets Are Evolving in Support of Broader GRC Management

Tom Eid, French Caldwell

Governance, risk and compliance (GRC) technologies must perform one or more of four critical functions: status and reporting, analysis and discovery, documentation, or controls automation and monitoring. If GRC technology or service providers cannot explain how they support one of those four elements of GRC technology, then it's not GRC technology. Finance and audit GRC provides the management, measurement, monitoring, auditing, automation and reporting of financial controls.

Key Findings

- Total software revenue for the finance and audit GRC markets in 2006 was $354 million worldwide and is forecast to grow to $893 million worldwide by 2011, a compound annual growth rate of 20.3%.
- As this marketplace continues to develop, it is about to shift from a high-growth phase to a consolidation phase, marked by frequent merger-and-acquisition activity and technology convergence.
- While the market is transitioning from best-of-breed and point products to broader suite/platform offerings, most initial purchases focus on financial controls and documentation of related internal controls.
- The European and Asia/Pacific regional markets will experience increasing spending growth as more organizations respond to financial compliance regulations such as "J-SOX" in Japan and "Euro-SOX" in the European Union, as well as other types of commercial compliance regulations.

Recommendations

- Determine your products' best fit within the finance and audit GRC marketplace; a "one size fits all" approach does not exist, and offerings must be tailored in appropriate ways, such as for documentation and reporting, segregation of duties, and audit.
- Vendors in the finance and audit GRC marketplace should target the office of the CFO and internal audit organizations as the primary buyers, but should not neglect key influencers such as the office of the CIO, the chief risk officer and the chief compliance officer.

- To establish a position as a leading GRC provider, consider acquisitions or developments for the related IT GRC, risk management, and legal and regulatory information governance marketplaces
- 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.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

WHAT YOU NEED TO KNOW

Most GRC technologies are focused on compliance, and some target risk management. Governance is set by corporate policy, law or other binding requirements. Compliance with those policies and laws can to some extent be automated, as can reporting against the objectives. Risk management, monitoring and analysis to some extent can also be automated — although much of the assessment of risks is a heuristic exercise that remains manual in the extreme.

Thus, most GRC technologies are really gRC (small g, big R and big C), with the "g" element limited to the management of policies and mapping of those against risks and controls. The purpose of these technologies is to reduce the burden of compliance (that is, to loosen the chains that restrict freedom of action) and to improve operational performance, not just to obtain better governance.

Many applications that can support compliance have been in use well before the current compliance wave. Examples include e-mail archiving, records management, workflow, identity and access management, change management, and configuration management. Any software that provides improved process management, automation, monitoring, reporting and auditing could be relevant to compliance. As a software vendor or service provider, determine how your products and offerings can be used to:

- Document records, reports and audits
- Automate reporting and workflow, testing of controls, the controls themselves, the process, or the work that is being controlled
- Analyze transactions, interactions and human behavior
- Monitor controls, changes and events

These functions are important to shifting from manual process controls to automated system controls and, thus, reducing labor components of compliance and risk management costs, including management time and attention, required to ensure compliance.

Technology can be used not only to document and automate; increasingly, it can be used also to generate documentation on the existing baseline and to provide measures of performance. A growing variety of monitoring technologies in multiple contexts can automatically identify violations of policy and changes in the baseline. Analysis technology presents status information in a variety of ways, from summary dashboards to detailed investigative reports.

Most businesses are adopting a three-phase strategy for investing in IT support for compliance activities:

- Phase 1 (reactive and one-off implementations) is just about complete.
- Phase 2 (proactive, coordinated implementation) is under way and will continue through the end of 2008.
- Phase 3 (automated processes and integrated compliance) will then follow and continue in best-practice mode.

Software vendors and some organizations are laying the foundation for an integrated compliance and operational risk architecture. This architecture will enable the elimination of some compliance process controls because equivalent system controls will be inherent in the evolving architecture. Businesses will also be capable of eliminating numerous compliance-specific applications for

audit, disclosure and financial controls because financial applications will incorporate and support the same functionality. The net result for businesses will involve a reduction in the total cost of compliance.

Recommendations for Software and IT Services Providers

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

- Determine your products' best fit within the finance and audit GRC marketplace; a "one size fits all" approach does not exist, and offerings must be tailored in appropriate ways, such as documentation and reporting, segregation of duties, and audit.
- Implement a well-integrated suite of products with seamless navigation and information, and context transfer between internal components and external applications. GRC management and controls automation, 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 partnering to fill functionality gaps. Seek partnerships and software components that support audit management, audit data extraction and analysis, segregation of duties, and business rules management.
- Ensure your ability to integrate with the GRC offerings of major platform vendors, such as SAP and Oracle, as well as IT services management vendors, such as IBM, BMC Software, HP and CA.
- Establish subject matter expertise regarding use cases, best practices and thought leadership within your service organization and through your software.
- Examine partnerships with system integrators for implementation expertise.
- To establish a position as a leading GRC provider, consider acquisitions or developments for the related IT GRC, risk management, and legal and regulatory information governance marketplaces
- 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.

Recommendations for Vendors When Working With Business Users and IT Organizations

If you are a software vendor or service provider, when working with a user or a member of an IT organization:

- Show how your products' and services' support for compliance with the U.S. Sarbanes-Oxley Act of 2002 (SOX) and related regional regulations, as well as extensibility to other forms of compliance and regulations and to general risk management, is a benefit for commercial and organizational uses.
- Help 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.

- Demonstrate the ability to automate the execution of repetitious control functions and focus on aggregating common control features that leverage your financial control framework.
- Support the implementation of a strategic, phased approach, because more investments are required to deploy new solutions and retrofit established systems.
- Target the office of the CFO and internal audit organizations as the primary buyers, but do not neglect key influencers, such as the office of the CIO, the chief risk officer and the chief compliance officer.

ANALYSIS

Software Vendor Taxonomy

The terms 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 adopted a specific marketplace terminology for these general terms, as governance, risk and compliance (or GRC). Governance, risk management and compliance have many valid definitions. The following definitions illustrate the relationship of the three terms and serve for Gartner's compliance and risk management research:

- *Governance* — The process by which policies are set and decision making is executed.
- *Risk management* — The process for ensuring that important business processes and behaviors remain within the tolerances associated with those policies and decisions, going beyond which creates an unacceptable potential for loss.
- *Compliance* — The process of adherence to policies and decisions. Policies can be derived from internal directives, procedures and requirements, or external laws, regulations, standards and agreements.

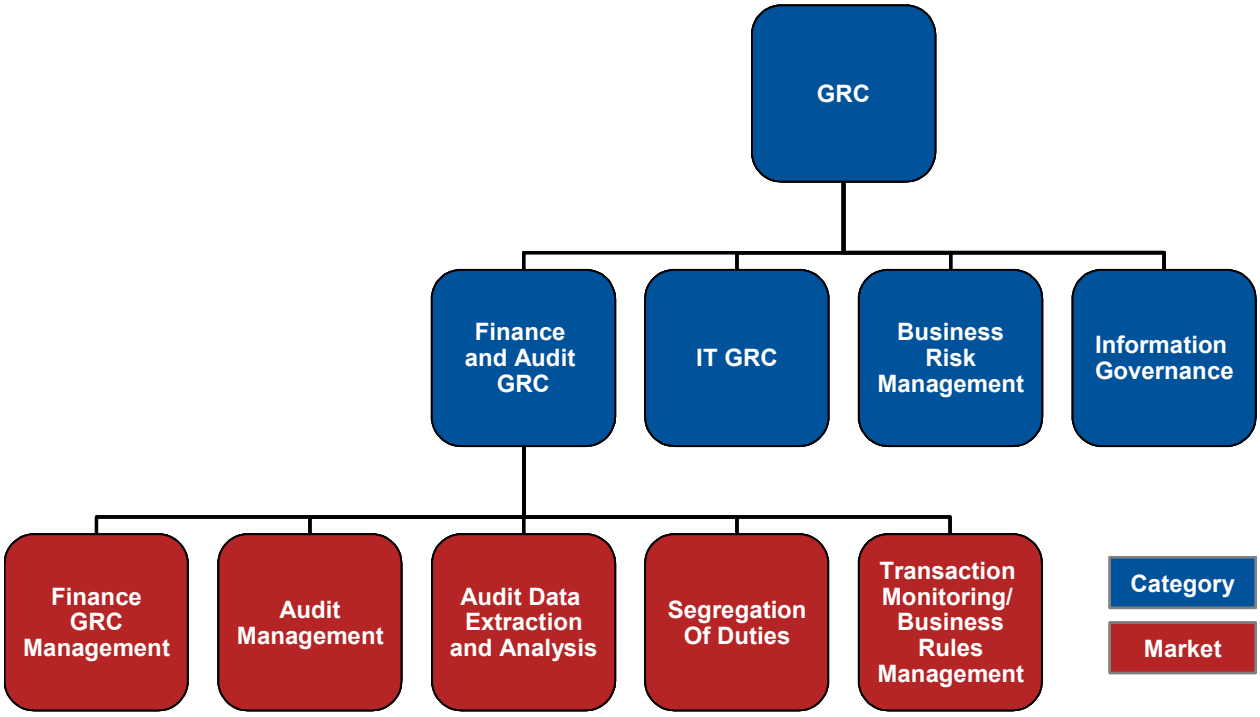
As used in this report, GRC is a selective focus that concerns the use of content management, compliance reporting, workflow and controls automation technologies, among other software products, to be used in support of audit, financial management controls, operational risk management (including compliance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

IT services and technology can support three different GRC objectives: efficient and effective operations, financial reporting accuracy, and compliance with policies, laws, regulations, and other binding requirements, such as service-level agreements and contracts. All these are business goals, and to ensure that IT processes are effective in enabling them, IT goals should be aligned with those business goals.

Software offerings in the GRC marketplace are aligned to categories and software markets. There are four GRC categories with multiple software markets aligned to each category, as shown in Figure 1:

- Finance and audit GRC — Markets include audit management, audit data extraction and analysis, business rules management, finance GRC management, and segregation of duties.
- IT GRC — Markets include IT GRC management, configuration auditing, log analysis/secure event and information management, and access management.
- Business risk management — Markets include Basel II risk management, operation risk management and risk assessment.
- Legal and regulatory information governance — Markets focus on active policy management, content monitoring and filtering, e-discovery, records management, e-mail archiving, and spreadsheet controls.

Figure 1. Finance and Audit GRC Management Software Markets



Source: Gartner (November 2007)

This report focuses on finance and audit GRC software, which includes software for finance management GRC, audit management, audit data extraction and analysis, segregation of duties, and business rules management. A representative alphabetical listing of vendors providing related software products is presented in Table 1.

Table 1. Alphabetical Listing of Vendors Providing Related Software Products

Category	Business View	Representative Vendors
Finance GRC Management	Management, workflow, documentation and reporting associated with financial controls	Achiever Business Solutions, Axentis, BI International, Bwise, Cura, MetricStream, Movaris, onProject, OpenPages, Oracle, Qumas, Paisley Consulting, SAP, Securac
Audit Management	Internal audit work papers, task management and workflow	Methodware, Paisley Consulting, Wolters Kluwer (TeamMate, acquired from PricewaterhouseCoopers)
Audit Data Extraction and Analysis	Tools for extracting data from business applications and running ad hoc analysis or templated queries	ACL, Oversight Systems, CaseWare IDEA
Segregation of Duties	Ensuring that personnel do not have access to data in a way that creates the potential for fraud	ACL, Approva, Oracle (Applimation, LogicalApps), Oversight Systems, Phulaxis, SAP
Business Rules Management	Monitoring transactional data in accordance with business rules established as controls	170 Systems, CODA, Infogix, Trintech

Source: Gartner (November 2007)

Software products for continuous automation and monitoring are included in the categories of segregation of duties, audit data extraction and analysis, and business rules management. While they focus on those functions and activities where 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, business process management, enterprise content management, human resource management, IT operations management, policy enforcement, and IT security.

Finance and Audit GRC Software Forecast

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

This forecast updates the forecast in the report "Finance and Audit GRC Market Is Expanding." This forecast includes total software revenue for finance and audit GRC software (see Table 2).

Table 2. Finance and Audit GRC Management Software Forecast, Worldwide Total Software Revenue, 2006-2011 (Millions of Dollars)

	2006	2007	2008	2009	2010	2011	CAGR (%) 2006-2011
Total Software Spending	**353.9**	**460.3**	**566.5**	**672.6**	**780.9**	**893.1**	**20.3**

	2006	2007	2008	2009	2010	2011	CAGR (%) 2006-2011
Note: Gartner Dataquest defines total software revenue as revenue generated from new licenses, updates, upgrades, subscriptions and hosting, technical support, and maintenance. Professional services, training and certification, and hardware revenue are not included in total software revenue.							

Source: Gartner (November 2007)

Many organizations are now establishing an overarching 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 above 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.

BACKGROUND AND CONTEXT

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 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. Furthermore, in an emerging trend, many organizations that are not required by law to comply with SOX have implemented many of the requirements for internal controls in response to perceived business advantages and external auditors' higher standards.

In May 2006, the European Union promulgated a new 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. Credit rating agencies and listing exchanges are also raising the bar on financial controls and risk management.

THE IMPACT

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 a similarly fragmented IT and line-of-business management structure.

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, there is more emphasis 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.

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 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 some audit management, segregation of duties, and business rules management functionality.

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 finance and audit GRC 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 (Hyperion/Oracle and Business Objects/SAP) and small (Virsa/SAP, LogicalApps/Oracle) companies are beginning to create uncertainty about vendor selection and product offerings.
- Confusion about the overlap or lack thereof of large vendors' financial applications, GRC and business intelligence road maps.
- 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.

CONCLUSION

Many software vendors have jumped onto the SOX and compliance "bandwagon," touting comprehensive solutions. However, no single GRC software market exists. A GRC management market has emerged 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. By 2009, a GRC platform market could emerge that will integrate the decision support and reporting, more extensive risk management, controls automation and monitoring, and interfaces with financial and other business applications.

Software markets usually follow a fairly consistent series of phases, from embryonic to emerging, high growth, consolidation and maturity, and then decline. The GRC marketplace is in the high-growth phase and is about to make a transition to a consolidation 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/platform offerings. Recent examples of mergers and acquisitions include:

- Oracle acquiring PeopleSoft, Stellent, Hyperion and LogicalApps
- LogicalApps acquiring segregation-of-duties functionality from Applimation
- SAP acquiring Virsa Systems and Business Objects
- Securac acquiring Certus

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 appeared in 2006, and in Europe, where SOX-like regulations will be rolled out during the next several years. Vertical industries that are not covered by SOX, for example, government agencies and mutual insurance firms, are also rolling out SOX-like rules. Should risk management be widely adopted as a business improvement discipline, it would add additional momentum to the GRC marketplace.

RECOMMENDED READING

"Audits and Events Drive Governance, Risk and Compliance Spending"

"IT GRCM Functions Defined"

"Magic Quadrant for Finance Governance, Risk, and Compliance Management Software, 2007"

"Hype Cycle for Legal and Regulatory Information Governance, 2007"

"Hype Cycle for Compliance Technologies, 2007"

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

"The 2007 Compliance and Risk Management Planning Guidance: Governance Becomes Central"

This document is published in the following Market Insights:

Software Applications Worldwide
Software Infrastructure Worldwide

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
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509