13 July 2011

Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms

French Caldwell, Tom Scholtz, John Hagerty

The EGRC platform market has expanded from a tactical focus on regulatory compliance to a strategic focus on enterprise risk management. Many vendors are looking toward the next market phase, which includes adding or integrating with business performance management and scorecarding capabilities.

What You Need to Know

This Gartner Magic Quadrant for enterprise governance, risk and compliance (EGRC) platforms (see Note 1) presents a global view of Gartner's assessment of the main software vendors that should be considered by organizations seeking a technology solution to support the oversight and operation of enterprisewide risk management and compliance programs, with the overall objective being improvements in corporate governance and the ability to achieve business objectives.

Buyers should evaluate vendors in all four quadrants. The vendors from the Niche Players quadrant have the core functionality of an EGRC platform, and, while having some product or product strategy challenges, offer good value for money, specialized industry capabilities or both. They bring some unique approaches to the market that can be of value to many companies. Several vendors in the Visionaries quadrant are driving innovation in the market through integration with business process modeling, continuous controls monitoring (CCM), risk analytics, targeted vertical industry solutions, and other advanced capabilities beyond the core functions required to be in the Magic Quadrant. Leaders are innovating with advanced capabilities, have large customer bases, have solid capabilities in the core platform functions — audit management, compliance management, risk management and policy management — and have executed across several industries, with support for multiple professional roles. Challengers have executed well, but lag the Leaders in advancing their range of advanced GRC capabilities for specific industries or professional roles, or they have a functional or architectural challenge that should be closed.

The placement of the vendors and commentary in this Magic Quadrant (see Figure 1) are based on multiple sources. Customer perceptions of each vendor's strengths and challenges are derived from EGRC-related inquiries with Gartner, as well as an email survey of vendor customers conducted in March, April and May of 2011. The evaluations also have drawn from vendor briefings, a vendor-completed questionnaire about their EGRC platform strategies and operations, scripted product

demonstration sessions with vendors, and other publicly available and proprietary financial, product and vendor information.

Magic Quadrant

Figure 1. Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms

Source: Gartner (July 2011)

Market Overview

The EGRC Platform Market

The EGRC platform market derives from the need for many entities to improve the oversight of corporate governance — including financial reporting compliance, enterprise risk management (ERM) and related audits. Many organizations also want to consolidate other GRC activities into a common platform. Therefore, an EGRC platform must solve the immediate GRC management (GRCM) needs associated with corporate governance, and also enable an enterprise to pursue future consolidation and integration of a diverse set of GRC activities.

"GRCM" is defined as the automation of the management, measurement, remediation and reporting of controls and risks against objectives, in accordance with rules, regulations, standards, policies and business decisions. Many enterprises typically consider a GRCM application to satisfy a specific requirement, such as Sarbanes-

Oxley (SOX) compliance, an industry-specific regulation or operational risk management (ORM) for a business process. However, enterprises often have other GRCM activities in mind, such as audit management, additional regulations (see "Hype Cycle for Regulations and Related Standards, 2010"), IT governance, remediation management and policy management, which they eventually may integrate into a more consolidated EGRC approach. During the past two years, ERM has emerged as a leading reason for implementing an EGRC platform. Related to ERM, there is an emerging demand to link GRCM to business performance objectives.

Most enterprises are also looking for solutions that support their strategies for more controls automation, including reporting from CCM of ERP and other controls automation in the IT infrastructure that can be integrated into the EGRC platform. As a consequence, a trend of the convergence of CCM with the EGRC platform is emerging, and there is also a slow trend toward the convergence of IT GRCM and EGRC platform solutions. Some EGRC platform vendors are also starting to add content and capabilities to meet operational GRC needs, such as environmental, health and safety (EH&S) compliance and business continuity planning. Overall, EGRC platform vendors are adding capabilities across a wide spectrum of financial, IT, operational and legal needs.

Despite the efforts of EGRC platform vendors to satisfy as many GRC needs as possible, they tend to focus on cross-industry requirements, and many industry-specific GRC solutions will remain — for lack of a better term, these are called "operational GRC." One operational GRC market that is growing rapidly is the energy trading and risk management (ETRM) platform market (see "Magic Quadrant for Energy Trading and Risk Management Platforms"). Another example of operational GRC is the broad marketplace for financial services risk management solutions (see "A Banker's Guide to Credit, Market and Operational Risk Management Software Functionality"). Rather than try to replicate the capabilities of these specialized solutions, EGRC platform vendors most often are trying to integrate with them.

IT GRCM Offerings of EGRC Platform Vendors

EGRC platforms serve organizations that take an enterprise approach to compliance and risk management, and that want to have all business units, including the IT organization, on the same GRCM solution. Most vendors with EGRC platforms offer modest IT governance automation functions. At a minimum, EGRC vendors offer the capability to document, survey, and report IT risks and controls, but some may lack IT-specific content. Some vendors also provide support for an IT asset repository, IT policy management and the automated collection of IT controls data. Organizations with a primary interest in IT-centric GRCM requirements should be aware that most EGRC platforms balance finance, operational and IT requirements at the expense of IT-centric depth.

Gartner is monitoring the potential convergence of IT GRCM and EGRC functions, such that this differentiation would become generally irrelevant to the market; however, this has not yet happened in 2011. The most significant limiting factor is the divergence of requirements between top-down and bottom-up approaches (see Note 2). In many cases, organizations are buying two separate tools, indicating that this difference is more substantial than just vendor marketing and different buying centers.

This divergence is based on the differences in management and reporting requirements for top-down versus bottom-up approaches. Top-down requirements tend to be led by ERM teams addressing business executive requirements, as opposed to bottom-up requirements, which are typically led by IT or information security operations teams. The vendors continue to add functions that overlap top-down and bottom-up requirements,

but convergence will only happen when organizations stop buying multiple tools to address diverging requirements, and agree on one tool to address both approaches comprehensively.

Some EGRC platform vendors qualify as IT GRCM vendors. BWise, MetricStream and OpenPages are EGRC platform vendors that have added IT GRCM capabilities. Archer EMC-RSA is also an EGRC platform vendor, but it started in the IT GRCM market.

Key Trends Affecting the EGRC Platform Market

EGRC platform demand is increasing because of several emerging trends, which include:

- The SOX knock-on effect

- An increasingly professional customer base that wants better analytics and alignment to strategic business objectives

- An increasing regulatory focus on anti-corruption and bribery in the aftermath of the financial crisis

- ERM to support transparency objectives of regulators and decision making by business leaders

- Regulatory content services and change management to deal with regulatory proliferation

- Consolidation, with a shift from dominance of the market by smaller best-of-breed players to one dominated by large vendors

The SOX Knock-On Effect: Demand for GRC solutions is highest in the U.S., where corporate governance regulations are the most stringent. However, as other countries, such as Canada, Japan, India, Australia and South Africa, and members of the EU have begun to enforce similar regulations, demand has increased globally. For a list of corporate governance codes and regulations, see the "Appendix for Corporate Governance Reforms" in the University of Michigan study "Cross-Border Target Selection and Investor Protection Disparity." A knock-on effect from SOX is that auditors in many geographies where internal controls requirements may not be legally as stringent as in the U.S. are still raising the bar on internal controls for financial reporting for their clients. In 2011, this trend has shown up notably in inquiries from Scandinavia, Italy and the Middle East.

Anti-Corruption and Bribery: Compliance with new regulations as a result of the financial crisis (see "International Collaboration of Regulators Will Impact Financial Services Providers") and increased enforcement of regulations requiring more transparency in business relationships, such as the U.K. Bribery Act 2010 and the U.S. Foreign Corrupt Practices Act, are emerging as new drivers of GRC solutions.

Enterprise Risk Management: ERM has emerged as the most significant use of EGRC platforms. With the proliferation of regulations and concerns over corporate governance and transparency, ERM is seen by many regulators and business leaders as a strategic approach to achieve improved corporate governance, more transparency in the decision making of the board and senior executives, and improved performance against business objectives. In a 2011 survey of EGRC platform vendors' customers, 46% reported using the platform for ERM, 45% for compliance with SOX or similar laws, and 40% for audit management.

Regulatory Proliferation: With accelerating regulatory proliferation, new market demands are emerging, such as content services and regulatory change management. Customers are looking for vendors not just to provide content for standards, regulations and policies, but also to keep the content updated, manage content licenses, provide alerts when a new regulation or change to a regulation emerges, and provide analysis and policy changes based on the impact of the regulatory change. No vendor is fully addressing this level of content services, although the major regulatory content publishers (such as Thomson Reuters and Wolters Kluwer) have some solutions for the financial services industry that are relevant. Law firm Morrison Foerster has also entered the regulatory content service market, providing some notification and analysis services for its clients. Many EGRC platform vendors have responded with improvements in workflow and policy management to support regulatory change management, which can affect policies, risk assessments, controls and business processes. A few of the EGRC platform vendors, besides those regulatory content publishers, have engaged in partnerships with regulatory content publishers. Others are increasing their efforts at providing regulatory and standards content, but issues with keeping the content updated are not being well-addressed (see "Combine Content and Workflow to Optimize a GRC Solution for Your Company").

Risk Analytics: During the past several quarters, buyers have placed increasing emphasis on analytics in EGRC, especially at the intersection of risk management. This is a direct result of customer maturity. The bottom-up approach of managing compliance and measuring risk at each process or operations area is gradually being augmented with the necessary top-down perspective, where executives and managers quantitatively assess risk and compliance across the entire organization, making balanced decisions for the enterprise as a whole. Additionally, the increased availability of external data points enriches the analytic experience, and provides a strategic and holistic approach to risk-adjusted performance management. This trend does not spell the end to more tactical approaches to GRC — organizations move at different speeds — but it represents an expansion in criteria for a strategic EGRC system evaluation.

Market Consolidation: Consolidation in the EGRC platform market picked up in 2009 and continued into 2010. In 2010, IBM acquired OpenPages. In early 2010, Archer was acquired by EMC-RSA, and BPS and Resolver merged to form BPS Resolver. Paisley was acquired by Thomson Reuters in early 2009, and in the third week of July 2009, three acquisitions were announced: IDS Scheer by Software AG, Cura by SoftPro Systems, and Axentis by Wolters Kluwer. None of these acquisitions have had immediate impact on current customers; however, over the long run, it is important to ensure that the goals of the acquirer are in line with the original rationale of the solution buyer. Also, when the acquirer has other related GRC software and services, there is often a challenge in integrating them with the acquired EGRC platform.

Market Definition/Description

GRC as a marketplace can be broadly divided between GRCM products for the oversight and operation of risk management and compliance programs, and other GRC products for the automation and monitoring of controls. For a comprehensive description of the GRC marketplace, see "A Comparison Model for the GRC Marketplace, 2011 to 2013," which addresses the EGRC platform and its relationship to other GRCM markets, such as IT GRCM (see "MarketScope for IT Governance, Risk and Compliance Management"), ORM (see "Strategic Implications of Operational Risk Management Software Selection") and financial governance (see "Q&A: Current Issues in Financial Governance"). Each of these markets demands some of the functionality that is inherent in the

EGRC platform. Instead of acquiring separate solutions for finance, IT and other business units, many enterprises are choosing to use a single EGRC platform and, when necessary, integrating the many point and functional solutions to satisfy specific GRC needs. Reporting and managing through a single platform give executives, auditors and managers a holistic view of the enterprise's risk and compliance postures, as well as views sorted by requirement, entity and geography.

The primary purpose of the EGRC platform is to automate much of the work associated with the documentation and reporting of the risk management and compliance activities that are most closely associated with corporate governance and business objectives. The primary end users include internal auditors and the audit committee, risk and compliance managers, and accountable executives. The key functions of importance to these groups are:

- **Audit management:** Supports internal auditors in managing work papers, and scheduling audit-related tasks, time management and reporting.

- **Policy management:** Includes a specialized form of document management that enables the policy life cycle from creation to review, change and archiving of policies; mapping of policies to mandates and business objectives in one direction, and risks and controls in another; and distribution to and attestation by employees and business partners.

- **Compliance management:** Supports compliance professionals with the documentation, workflow, reporting and visualization of controls objectives, controls and associated risks, surveys and self-assessments, testing, and remediation. At a minimum, compliance management not only will include financial reporting compliance (SOX compliance), but also can support other types of compliance, such as ISO 9000, Payment Card Industry, industry-specific regulations, service-level agreements, trading partner requirements and compliance with internal policies.

- **Risk management:** Supports risk management professionals with the documentation, workflow, assessment and analysis, reporting, visualization, and remediation of risks. This component focuses on general ORM, but may collect data from specialized risk analytics tools to provide a consolidated view of ERM. Many industry-specific risk management requirements may not be supported. For example, many banks require highly specialized capabilities for Basel II compliance. Only a few EGRC platform vendors support the ORM needs of banking, and most vendors prefer to integrate the platform with specialized solutions from other vendors.

The EGRC platform can integrate with business applications, business intelligence (BI), enterprise content management, controls automation, monitoring solutions (such as segregation of duties), IT technical controls (such as server configuration auditing) and CCM for transactions. The EGRC platform also integrates with specialized GRCM solutions, such as EH&S compliance, quality management and industry GRCM applications.

For a comprehensive market description, see "The Enterprise Governance, Risk and Compliance Platform Defined."

Inclusion and Exclusion Criteria

Vendors were included in this Magic Quadrant if they met these criteria:

- Ability to deliver the four primary GRCM functions: audit management, compliance management, risk management and policy management.

- Credible presence in the marketplace: defined as having at least $11 million in annual revenue for calendar year 2010 from EGRC platform software, at least 50 customers, and customers able to be referenced for corporate-governance-related GRC activities, such as financial reporting compliance and ERM.

Vendors were excluded if they did not meet the functional, revenue and implementation criteria; did not have adequate referenceability; or were an industry-specific or highly specialized solution.

Added

- Aline changed its name to AlignAlytics

- Enablon met the inclusion requirements

- IBM acquired OpenPages

- Strategic Thought Group changed its name to Active Risk

Dropped

- Protiviti's EGRC platform revenue fell below the increased threshold for the 2011 Magic Quadrant.

- Wolters Kluwer shifted its marketing and product strategies to de-emphasize integration of its various GRC-related products.

Evaluation Criteria

Ability to Execute

Vendors are assessed on their ability and success in making their vision a market reality. The following six Gartner criteria for Ability to Execute were considered:

- **Product/Service:** Core goods and services offered by the provider that competes in/serves the defined market. This includes current product/service capabilities, quality, feature sets and skills, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria. Vendors were evaluated primarily on effective provisioning of the four primary functions — audit management, compliance, risk management and policy management. Ability to support IT GRCM was also an element.

- **Overall Viability:** Includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood of the business unit to continue to invest in the product, offer the product and advance the state of the art in the organization's portfolio of products. Overall company revenue and revenue from the EGRC platform were the key determinants.

- **Market Responsiveness and Track Record:** Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. A key metric was sales performance in 2009 and the first quarter of 2010, a very challenging period for the IT industry.

- **Sales Execution/Pricing:** The technology providers' capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel. For sales execution, a key metric was the size of the EGRC platform customer base. For pricing, key metrics were transparency and ease of calculation of the pricing model.

- **Customer Experience:** Relationships, products and services/programs that enable customers to be successful with the products evaluated. Customers were asked a variety of questions to determine their experience with the vendor and the EGRC platform, including whether the product met, exceeded or failed to meet expectations, areas where the vendor should improve, and the overall level of satisfaction with the vendor. Key metrics included overall satisfaction, breadth of use, ability to meet performance expectations, and negative comments from reference customers.

- **Operations:** The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure — including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis. Key metrics were the experience of senior management and turnover of senior management.

There have been no changes in the criteria weights since the 2010 Magic Quadrant.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	Standard
Overall Viability (Business Unit, Financial, Strategy, Organization)	Standard
Sales Execution/Pricing	Standard
Market Responsiveness and Track Record	High
Marketing Execution	No Rating
Customer Experience	Standard
Operations	Low

Source: Gartner (July 2011)

Completeness of Vision

Vendors are rated on their understanding of how market forces can be exploited to create value for customers and opportunity for themselves. The following six criteria for Completeness of Vision (see Table 2) were considered significant for the EGRC platform market:

- **Market Understanding:** Ability of the provider to understand buyer needs and translate these needs into products and services. Vendors that show the highest degree of vision listen to and understand buyer wants and needs, and can shape or enhance those wants with their added vision. Vendors understood major EGRC platform trends, particularly the relationship of ERM to business performance.

- **Marketing Strategy:** A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements. EGRC platform vendors were evaluated on whether their strategies were clearly consistent and aligned with market direction.

- **Offering (Product) Strategy:** A provider's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature set as they map to current and future requirements. EGRC platform vendors were evaluated on whether they were closing any significant product gaps, the ability to address a variety of use cases with core and advanced capabilities, and their GRC content strategy.

- **Vertical/Industry Strategy:** The provider's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical industries. EGRC platform vendors were evaluated on whether they had differentiated offerings for two or more highly regulated industries, could meet the ORM needs of the financial services industry, and had content and capabilities for industry-specific needs.

- **Innovation:** Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, and defensive or pre-emptive purposes. The primary metrics for EGRC vendors were R&D investment and significant noncore capabilities.

- **Geographic Strategy:** The provider's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside its native geography — directly or through partners, channels and subsidiaries — as appropriate for that geography and market. The primary metrics were direct sales and support presence in multiple geographies, and reseller and service partner support.

There have been no changes in the criteria weights since the 2010 Magic Quadrant.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	Standard
Marketing Strategy	Standard
Sales Strategy	No Rating
Offering (Product) Strategy	High
Business Model	No Rating
Vertical/Industry Strategy	Standard
Innovation	Standard
Geographic Strategy	Low

Source: Gartner (July 2011)

Leaders

The EGRC platform market is consolidating, and the vendors in this market have had time to develop their products and strategies. Customers are looking for Leaders to provide additional functionality, such as support for chief risk officers, integration with advanced BI and corporate performance management applications, business process modeling, more-flexible and ad hoc reporting, planning and resource management for internal audit, and content and specialized capabilities for risk management and compliance beyond the core functions, such as CCM. They also expect support across multiple geographies. The large vendors should be best positioned for these requirements, yet smaller vendors are in the Leaders quadrant because of continued viability, more-advanced functionality and market understanding.

Challengers

Challengers have proven viability, demonstrated market performance and the ability to exceed customer expectations on technical functionality. Challengers need to focus on their product road maps, as well as their sales, marketing, geographic and vertical industry strategies to move into the Leaders quadrant.

In last year's Magic Quadrant, there were a large number of Challengers. In this Magic Quadrant, two of them, Oracle and Thomson Reuters, moved into the Leaders quadrant. Both are large vendors that had been focused on organizational or architectural issues associated with the EGRC platform acquisitions they had made. They have now resolved those issues and are refocused on their marketing and product strategies. Some other Challengers in the 2010 Magic Quadrant moved to the Visionaries or the Niche Players quadrants, with Ability to

Execute being challenged by increasing customer demands for more advanced functionality in a consolidating market.

Visionaries

Visionaries have a solid understanding of the market, as demonstrated by domain expertise and responsiveness to customer expectations. They are actively executing against an aggressive product road map that expands support to additional regulatory and nonregulatory compliance and risk management needs, including support for the integration of GRC with business performance. In a consolidating market, smaller Visionaries will have to differentiate themselves with advanced functionality to remain competitive.

Niche Players

Niche Players often have a unique approach to the market. Vendors could also be in the Niche Players quadrant because they have to improve the core platform functions. Niche Players may also target a specific industry vertical or the needs of particular professionals. All vendors in the Niche Players quadrant are successful in the market with competitive solutions.

Vendor Strengths and Cautions

Achiever (Sword Group)

Sword Group demonstrated Sword Achiever version 4, released February 2011. It has the core functionality required for an EGRC platform, but Sword Group has had challenges in extending its customer base beyond Achiever's legacy as an operational GRC offering focused on compliance with International Organization for Standardization (ISO) standards and EH&S. Sword Achiever has a rapid release schedule and executes well against its road map. Sword Group is in the Niche Players quadrant. To improve competitiveness in the EGRC platform marketplace, Sword Group must direct future releases to include more advanced risk management and compliance functionality, and close gaps in its domain knowledge for ERM and financial GRC.

Strengths

- Product Strategy — Sword Achiever has strengths in EH&S and ISO standards compliance for manufacturing and other process industries.

- Innovation — A high percentage of revenue is invested in R&D, and frequent updates are made to improve the product.

- Product — Being based on .NET and with SharePoint integrated, Sword Achiever has good policy life cycle management capability and reasonable audit management. Survey respondents noted audit management, policy management and EH&S compliance as their most common uses for the platform.

Cautions

- Market Understanding — Sword Achiever did not demonstrate a deep understanding of ERM and trends toward integration of risk management and performance management.

- Product — Audit management was weak on risk-based scoping of the audit universe. Compliance and risk management functions were basic.

- Operations — Domain expertise beyond operational GRC, such as ISO compliance and quality management, needs to be improved.

Active Risk

Active Risk demonstrated Active Risk Manager version 5.0, which was released in January 2011. Active Risk has strong capabilities in ORM, including quantitative risk analytics and Monte Carlo simulation, and it focuses on industries with heavy infrastructure investments. Active Risk also has solid capabilities in the other core functions. Active Risk has moved from the Niche Players to the Visionaries quadrant based on advanced functionality, which indicates a solid understanding of the market and a strong vertical strategy.

Strengths

- Market Understanding and Strategy — Active Risk has a practical, risk-based, closed-loop process approach that is focused on risk-adjusted investment decision making and risk evaluation for other corporate business objectives. Its market approach is in line with the trend toward ERM in most industries.

- Product Strategy — Active Risk is very focused on ongoing improvement of risk management functionality and integration with other enterprise applications to collect data in support of risk-based decision making or risk intelligence. It can address a large number of compliance use cases, but is directed toward the operational compliance needs of heavy infrastructure industries.

- Vertical/Industry Strategy — Active Risk addresses the needs of manufacturing, aerospace and defense, nuclear, construction and engineering, and mining industries, as well as government agencies that are aligned with those industries through contracting or oversight. The vendor intentionally is not focused on banking.

- Product — Active Risk has good overall functionality for the primary EGRC platform functions, with strength in risk management. It offers quantitative risk analysis, including a Monte Carlo simulation engine for risk scenario analysis and investment decision making. It has a closed-loop process for the analysis of insurable losses, root cause analysis and optimization. The process includes calculating ROI from risk-adjusted corporate performance. Active Risk has one of the better integrations of performance management and risk management capabilities. It is one of two EGRC platform vendors that support entity management.

Cautions

- Product — Customer references noted that they would like to see improvements in quantitative risk management and reporting integration with office productivity software.

- Product Strategy — Active Risk offers no vendor-provided or licensed content, although it is assessing adding content in future versions.

- Vertical/Industry Strategy — Active Risk specifically avoids banking, but with its focus on managing insurable risks and the market opportunity of Solvency II, it is starting to work with insurance firms. Avoiding the banking industry is not a long-term viable strategy for the EGRC platform market, and, interestingly, it has the functionality to support ORM for financial services.

AlignAlytics

AlignAlytics (formerly Aline) offers a SaaS-based GRC product suite. The release demonstrated became available in January 2011. AlignAlytics moved from the Challengers to the Niche Players quadrant this year as a result of its product focus shift to emphasize the risk-to-performance connection. Although this move is in line with the market demands for functionality to align risk and performance management, AlignAlytics has shifted its strategy so far toward performance that its commitment to traditional GRC needs, such as compliance, ORM and audit management, is heavily de-emphasized. This repositioning also is reflected in the company's new name (February 2011).

Strengths

- Market Understanding and Strategy — AlignAlytics has made a strategic decision to focus even more heavily on the risk and performance aspects of EGRC. The company's legacy is in the analytics and reporting arena, with thought leadership demonstrated throughout the past 15 years. Although this is not a major departure from its prior direction, it's not minor either. This is the primary reason why the suite is again considered a niche offering.

- Product — Compliance management, which is reasonable with good scoping features, is well-received by customers. Customers report that they use this product for financial compliance initiatives, specifically supporting SOX. Use of open-source capabilities for content management supporting policy management shows decent progress.

- Customer Experience — Customers are very satisfied, with expectations largely exceeded and no negative comments.

- Sales Execution — References report that AlignAlytics is a value-priced product, with the majority of respondents indicating that the product is less expensive than the competition's offerings.

- Operations — The management team is experienced and stable.

Cautions

- Product Strategy — The company is veering quite sharply toward its revamped risk-to-performance position, which leads us to believe that it may not be as committed to many other core EGRC functions going forward.

- Vertical Industry Strategy — There continues to be no evidence of a vertical industry strategy.

- Innovation — R&D investment is reported at 12% of revenue and remains below the average for small vendors.

- Customer Experience — Customers reported relatively constrained use of the product for SOX compliance, risk management and audit management.

- Geographic Strategy — AlignAlytics has moved beyond the U.S., with limited presence in the U.K., but the company is largely North American-based.

- Product — Audit management is weak, with noted gaps in work paper management and auditor time and expense reporting. Additionally, there is limited capability for policy management.

Archer (EMC-RSA)

EMC-RSA offers the RSA Archer eGRC Platform. The release demonstrated was version 5.0, which became available in December 2010. Despite being managed by RSA, The Security Division of EMC, Archer is getting good market response from non-IT customers. With Archer's IT GRC heritage, EMC-RSA is rated highly in the IT GRCM MarketScope. Having made its first new major release since its acquisition of Archer, and having maintained ongoing growth in sales, EMC-RSA stays in the Challengers quadrant.

Strengths

- Product Strategy — The RSA Archer eGRC Platform enables EMC-RSA to support a breadth of use cases beyond the standard risk management and compliance cases through customer self-development and sharing between customers in the Archer Exchange community, and through the development of new capabilities by EMC-RSA. Content is a strength of Archer's, and EMC-RSA is adding additional content to support more vertical industry and compliance needs.

- Product — The RSA Archer eGRC Platform has substantial capabilities in the four core EGRC platform functions. Advanced capabilities include loss event and root cause analysis features that are helpful in optimizing risk management and compliance processes. They are suitable for nonfinancial service applications, but are not used as much for financial services' specific requirements for ORM. The company offers support for content such as Basel II. Incident management supports a basic investigation capability — it suits ethics and other HR-related investigations well. RSA Archer is rated highly for IT GRCM.

- Overall Viability — The overall viability is much improved because of the acquisition of Archer by EMC-RSA in early 2010.

- Market Responsiveness — It has strong year-over-year growth in customers.

- Pricing — It has an easy-to-understand pricing model and per-module annual license for unlimited enterprise use.

- Customer Experience — Customers use RSA Archer for a wide range of GRC activities.

Cautions

- Market Understanding and Strategy — For EGRC, EMC-RSA needs to present more emphasis on the relationship of risk management to strategic objectives and business performance.

- Innovation — Archer had a history of not meeting its release dates. Ongoing investment by EMC-RSA is expected to improve its ability to meet release dates.

- Product — Although Archer is a strong competitor in the IT GRCM market in which automated controls data collection is a requirement, customer references stated that they would like to see improvements in data collection from automated controls.

- Pricing — Although the annual license, enterprise pricing model is transparent, customer references noted a lack of flexibility in pricing for variable use versus competitors' use.

- Customer Experience — Reference customers complain about a decline in responsiveness and communication since the acquisition by EMC-RSA.

BPS Resolver

BPS Resolver demonstrated BPS Resolver GRC Suite. BPS Resolver demonstrated good capabilities for audit management, compliance management and risk management. Policy management is limited. It is still a relatively small player in the market, with most of its revenue coming from North America. BPS Resolver remains in the Niche Players quadrant, mainly due to being slow to bring together the separate technology stacks for BPS and Resolver.

Strengths

- Market Understanding and Strategy — BPS Resolver has a good understanding of customer needs for ERM, as well as some specialized industry compliance requirements.

- Product Strategy — Primary EGRC platform capabilities are in place. Its focus during the next several months includes improving the workflow capabilities, instituting an online peer user network (Community) and refining its reporting functionality.

- Vertical/Industry Strategy — BPS Resolver targets multiple vertical industries, and it has developed specialized capabilities for some compliance challenges in healthcare and utilities. Specific support for healthcare compliance exists, particularly with Centers for Medicare & Medicaid Services (CMS) and Recovery Audit Contractors (RACs). BPS Resolver also supports electrical utilities' compliance with NERC-CIP.

- Innovation — It has some innovative solutions, such as electronic meeting balloting, which can be used for risk assessments. It has a high budget for R&D.

- Product — Content includes a stock library of risks. It offers excellent reporting through a spreadsheet-like matrix that can be taken offline. It also offers very good incident management, above-average survey functionality, and great notification capability through Outlook integration.

- Customer Experience — Reference clients report a high level of responsiveness, including a keen willingness to implement product improvements based on client feedback.

Cautions

- Market Understanding and Strategy — Although BPS Resolver has some business performance capabilities, business performance is not an explicit element of its GRC strategy.

- Product — The underlying architecture for a combined implementation of BPS and Resolver is based on two product stacks for now. Customer references stated that they would like to see improvements in workflow and audit management (GRC Cloud 5.5, released in July 2011, has improved workflow capabilities). Policy management is a challenge because of a lack of underlying content management.

- Geographic Strategy — BPS Resolver has no direct presence outside of North America, but it is adding partners in several regions.

BWise

BWise demonstrated version 4.1 SP-2, which was released in December 2010. BWise's position in the Leaders quadrant is based on a mature EGRC platform, to which BWise continues to add more-advanced capabilities, a large customer base and relatively high revenue, an experienced management team, and an innovative product strategy. It is the only vendor besides the large ERP vendors to offer an organic CCM solution that integrates with its EGRC platform. BWise is also included in the IT GRCM MarketScope (see "MarketScope for IT Governance, Risk and Compliance Management").

Strengths

- Market Understanding and Strategy — BWise has a solid understanding of the market for the integration of risk management and performance management, as well as a strong business process orientation.

- Product Strategy — Its road map emphasizes improvement in audit management and quantitative risk analysis, with consideration for customers needing credit and market risk management capabilities. BWise is focusing on enhancing its data analysis for audit and risk management, usability and offline capabilities.

- Vertical/Industry Strategy — BWise is well-positioned for financial services. It also has a risk library targeted at other vertical industries, such as energy, government and transport.

- Innovation — BWise is challenging the large ERP vendors by adding CCM to its EGRC platform.

- Geographic Strategy — It is continuing to expand beyond its home base in the Netherlands, with a large presence in North America and additional capability in the U.K., France and German-speaking countries. Other geographies are covered through partnerships.

- Product — BWise has strong capabilities in compliance management and risk management, with both qualitative and quantitative capabilities. It has solid loss event and root cause analysis, with an integrated Monte Carlo engine from its partner, Rogue Wave Software. Its platform includes a business process modeling capability to document and visualize business processes, risks and controls. Audit management, scheduling and planning have been improved. An optional CCM capability is also available. It is one of two EGRC platform vendors that support entity management.

- Operations — BWise has a stable, experienced management team.

Cautions

- Product — Reference customers reported that product functionality mostly "met expectations." They cited policy management and integration with external reporting tools as areas for improvement: The recent versions of BWise support effective integration with external reporting tools.

- Sales Execution — Outside of Europe and North America, direct sales are limited.

Cura Technologies

Cura Technologies demonstrated Cura Enterprise, version 3.6.4, which was released in January 2011. Since 2010, Cura has focused on improving the usability aspect of the product (survey management and reporting) and integration. The version demonstrated was an evolutionary upgrade from last year's demonstration. The move from the Challengers to the Visionaries quadrant reflects Cura having more clarity around its marketing strategy, but also the ongoing challenges in gaining traction in the primary EGRC markets of North America and Europe.

Strengths

- Vertical/Industry Strategy — Cura has good support for the financial services, pharmaceutical and process industries that have a lot of investment focused on major projects.

- Geographic Strategy — Cura has direct support in North America, Europe, South Africa and Australia.

- Product — It is very strong in risk management, with solid capabilities for qualitative and quantitative analysis, including Monte Carlo simulation. Cura is capable of broad ERM and ORM for financial services, and is particularly well-suited for project risk management. It provides a lot of content in its knowledgebases. In South Africa, Cura has teamed with LexisNexis to provide regulatory content feeds.

- Market Responsiveness — It has a large customer base and ongoing growth year over year.

- Pricing — Its very practical per-module and per-user pricing model is easy to calculate and compare. Reference clients indicate that Cura's pricing is very competitive.

- Customer Experience — References indicate that Cura exceeds expectations for ERM, and general satisfaction with Cura is high.

Cautions

- Marketing Understanding and Strategy — Cura's marketing message is confusing and diffuse. The acquisition by SoftPro Systems, while providing more investment, so far, has not helped Cura to develop a more focused marketing strategy.

- Product — Reporting has been an issue. Some evidence exists of challenges in supporting roll-up and reporting for large multi-entity enterprises. Recently, adding integration with BusinessObjects is beginning to close the gap. Cura needs to improve the policy management focus of its offering.

- Customer Experience — The customer references were primarily focused on risk management, and use for compliance management was less evident.

- Geographic Strategy — The majority of clients are still outside of Europe and North America.

Enablon

This is the first year that Enablon is included in the Magic Quadrant. Enablon has had EGRC functionality for a few years and now meets the Magic Quadrant inclusion criteria for revenue and number of customers. It

demonstrated Enablon 5.7, along with audit, compliance, risk and policy management modules. With global headquarters in Paris, a North American headquarters in Chicago, and a direct presence in the U.K. and Spain, its foundations are in operational GRC, with solutions for EH&S, quality management, and corporate sustainability performance management. Having the foundational functionality for EGRC, growing EGRC sales and a large customer base that already uses its platform for operational GRC, Enablon is positioned in the Challengers quadrant.

Strengths

- Product — Enablon has solid content on the sustainability aspects of corporate governance. Compliance management is strong, with advanced remediation and incident management features.

- Sales Execution — Enablon has a big customer base (more than 250) that forms a solid foundation into which additional GRC modules can be sold.

Cautions

- Customer Experience — Reference clients would like more freedom to customize screen layouts, something that Enablon is addressing in the latest versions of its solutions.

- Product — Reference clients indicate a need for more content about risk and compliance standards, as well as for questionnaires and assessments (which Enablon is starting to address via new content partnerships). Functionality for audit planning, work paper management, and time and expense control can be improved, and are part of the vendor's 2011 road map.

- Geographic Strategy — 80% of Enablon's revenue comes from Europe and the U.S. It is focusing on establishing its Asia/Pacific presence during 2011.

LogicManager

LogicManager demonstrated version 3.6.8. The company has been a 100% SaaS offering, although it has recently begun to offer an on-premises option, and has a strong focus on the integration of ERM with business performance. LogicManager is well-positioned to take advantage of growing interest in EGRC platforms by small and midsize companies. LogicManager's position in the Niche Players quadrant is based on some gaps, primarily in compliance and policy management, and in revenue, which affect its overall viability score.

Strengths

- Market Understanding — LogicManager supports a risk-based approach, with a strong linkage to performance management.

- Product — The linkage of risk management to performance management is a key differentiator. LogicManager also provides risk, compliance and policy libraries. Customer references noted that the functionality for ERM and third-party risk management exceeded expectations.

- Sales Execution — LogicManager has a very large customer base; however, based on estimated revenue, most sales are very small.

- Market Responsiveness — The SaaS delivery model is attractive to many companies seeking to minimize upfront costs, especially small and midsize businesses — many of which are just entering the market. LogicManager claims more than 400 new customers in 2010.

- Pricing — It has a simple-to-understand, per-user SaaS pricing model and has recently introduced an on-premises perpetual license model.

- Customer Experience — Most customers were satisfied with applying the product to several different GRC activities, with some stating that it exceeded expectations.

Cautions

- Product — Although LogicManager has a focus on linking risk management and performance management, risk management functionality is basic, as is audit management. Compliance and policy management are below average.

- Product Strategy — No evidence exists in LogicManager's road map that it is closing gaps in core functionality.

- Geographic Strategy — The company is focused on North America only.

- Overall Viability — LogicManager would not share revenue information. This lack of transparency in small vendors can be cause for concern.

Mega

Mega demonstrated its Mega Suite, version 3.3, which was released in December 2010. Mega remains in the Visionaries quadrant. With roots in the business process analysis and enterprise architecture markets, Mega can align a wide range of GRC activities with business objectives and processes. This alignment continues to provide a solid foundation for enterprise and operational risk management. As noted by references, time to deploy the solution can be long for customized implementations.

Strengths

- Market Understanding and Strategy — Mega's significant alignment of risk management to business process analysis complements well the market direction of risk management as a key component of business performance.

- Product Strategy — The company has completed the integration of its GRC offering with its business process analysis and enterprise architecture offerings. Mega has also completed its integration to SAP BusinessObjects for analysis and reporting of GRC activities and to provide a tighter link to business performance reporting.

- Vertical/Industry Strategy — Mega has a strong focus on banks and insurance, as well as growing emphasis on manufacturing, utilities and government. The company also targets its functions to specific business roles in its customers.

- Innovation — The company's road map for its GRC platform is scoped out through 2012, with several releases scheduled to deliver functionality in small bites for target industries and use cases. The company

spends a hefty amount on R&D, and expects to continue that level of funding. It has a comprehensive road map backed with solid investment. It has been innovative through integration with organic and partner capabilities to improve the business performance and ORM focus of its GRC platform.

- Geographic Strategy — Mega's direct sales and support coverage in multiple geographies continues to be extensive. It uses a broad network of channel partnerships to add more coverage.

- Product — Mega understands and executes successfully on audit, compliance and risk management capabilities. It also has partnered with a core set of providers to round out capabilities in the areas of risk analytics and risk content. These partnerships extend ORM capabilities. The company has also partnered with Approva for CCM.

Cautions

- Market Understanding and Strategy — Although we concur that a foundation of business process management and enterprise architecture can be compelling, sometimes buyers aren't looking to address those issues in the context of a GRC evaluation. The Mega product suite is modular, so there is no absolute need to use all components. Mega's reliance on those broader selling propositions can concern potential customers looking for direct solutions to specific issues and problems. We suggest that the company keep prospects' GRC pain points front and center.

- Market Responsiveness and Track Record — Mega has had a difficult time penetrating the North American market. Recent investments in GRC-experienced U.S.-based marketing and sales support should help.

Methodware (Jade)

Methodware, owned by Jade, demonstrated Enterprise Risk Assessor (ERA) Kairos, released in March 2011. Methodware offers a platform that is robust in audit, compliance and risk management capability. In this latest version, it has enhanced navigation and usability, but policy management, due for improvement in 2012, is still a challenge. It has a good understanding of ERM, but has yet to demonstrate product functionality that integrates risk management and business performance. Its marketing strategy seeks to add better support for financial services, and improved quantitative risk management is on the road map. With its marketing focus on financial services, but remaining gaps in functionality, Methodware has moved from the Challengers quadrant to the Visionaries quadrant.

Strengths

- Vertical/Industry Strategy — Methodware has a strong marketing focus on the financial services industry and core strengths in operational GRC, such as health and safety compliance.

- Geographic Strategy — It has a direct presence in North America, Europe, Australia and New Zealand, with partners for several other geographies.

- Product — It is strong in audit management, compliance and risk management. Scoping for audit and compliance is superb. It has very strong loss event and root cause analysis through integration with a partner's Monte Carlo simulation (Palisade @RISK). It has good integration with Microsoft Exchange for alerts and remediation tracking. The new version enables users to tailor their own workflows, called "Methods" by Methodware. Customer references noted that the ERM functionality exceeded expectations.

- Sales Execution — Methodware has a large and growing customer base.

- Market Responsiveness and Track Record — It continues to be a good value for small and midsize implementations, and is adding larger implementations as well.

- Customer Experience — Customer references indicated a high level of satisfaction with Methodware.

Cautions

- Vertical/Industry Strategy — Methodware is targeting financial services, but quantitative risk management improvement for financial services is in development.

- Product — It has poor policy management, which is not due for improvement until 2012. Customer references stated that they would like to see improvements in automated data collection, reporting and workflow — the latter two show significant improvement in the latest version.

MetricStream

MetricStream demonstrated the MetricStream GRC Platform, version 6.0, which was released in March 2010. MetricStream offers a highly competitive offering with all the core functionality and several advanced capabilities as well. MetricStream also is included in the IT GRCM MarketScope, and continues to improve its capabilities in that market. It is continuing execution against an aggressive road map.

Strengths

- Market Understanding and Strategy — MetricStream has a very good market understanding and strategy, with an integrated risk management and business performance orientation. It has a clear and consistent message, and targets organizations that are trying to meet multiple GRC objectives.

- Product Strategy — Its ongoing focus is on improving usability and navigation, business process integration, integration with CCM and automated IT controls, and content.

- Vertical/Industry Strategy — MetricStream targets highly regulated vertical markets with industry-specific content and functionality.

- Product — There are no gaps in its primary functionality for an EGRC platform. It has very strong audit management.

- Market Responsiveness and Track Record — MetricStream is very competitive, with solid, ongoing customer growth. Its development team is quick to create new capabilities based on market demand.

- Customer Experience — Customers indicated that the product met or exceeded their needs, and had a high degree of overall satisfaction.

Cautions

- Geographic Strategy — MetricStream has new customers in multiple geographies, but most of its direct presence is concentrated in North America and India. Recently, it established a small sales presence in Europe, and is strengthening its channel in EMEA and Latin America.

- Product — The product supports Oracle Database only. Reference clients would like to see improved workflow capability.

- Customer Experience — Reference clients of earlier versions indicate that out-of-the-box reporting could be improved to reduce the customization efforts required. For example, if standard reports include all fields, the user should be able to "scale back" by eliminating unneeded fields. Reporting functionality has been improved in the current version.

OpenPages (IBM)

OpenPages was acquired by IBM in 4Q10 and is part of the Business Analytics division of IBM's software group. The company demonstrated OpenPages 6.0, released in January 2011. OpenPages embarked on deeper integration with the IBM Cognos BI stack long before the acquisition was announced. As a result, analytics — risk analytics in particular — are a core strength of the product. The OpenPages platform has solid capabilities in all the core functions and above-average support for ERM and ORM. It continues to execute consistently on a well-planned road map. OpenPages remains in the Leaders quadrant.

Strengths

- Market Understanding and Strategy — OpenPages has a solid understanding of emerging markets for integrated GRC and business performance management. It has a comprehensive approach targeting multiple roles within the enterprise. The IBM link will only enhance this strategy.

- Product Strategy — No significant gaps exist in OpenPages' product strategy. Its enhancements for risk analytics and reporting integration for ORM demonstrate a trendsetting vision and have strengthened its offering.

- Product — OpenPages has particular strengths in audit management, risk management (including risk analytics) and policy management (including regulatory change management).

- Vertical/Industry Strategy — OpenPages has historically targeted the banking, insurance, energy and utilities markets with specific industry capabilities. It is also embarking on vertical presence in healthcare, with Medicare compliance, policy management and regulatory change management. It is expanding its horizon to other sectors, especially as the IBM channel kicks into gear.

- Operations — OpenPages has an experienced, established management team that has remained intact through initial phases of the IBM acquisition.

Cautions

- Geographic Strategy — As of today, OpenPages continues to compete in its historical markets of North America and Europe, along with a reseller relationship in Japan. The sales push from other geographies is now gearing up as part of the IBM Business Analytics integration and will take some time to mature.

- Offering Strategy — Integration into the IBM software stack is expected to take up development resources that might otherwise be used to enhance the product. Because OpenPages is aligned to the Business Analytics division of IBM, there is some concern that the company will less aggressively pursue non-analytics-based initiatives.

- Customer Experience — OpenPages continues to meet, but not exceed, the expectations of reference customers. Better reporting integration has been flagged by some references; part of the 6.0 release should address this concern.

Oracle

Oracle demonstrated Oracle GRC Suite 8.6, which was released in October 2010. Oracle has a vast technology portfolio spanning applications, middleware and hardware, and the company places strong emphasis on the integration of its EGRC platform, called Oracle Enterprise Governance, Risk and Compliance Manager, with other Oracle assets, such as Hyperion for financial close, reporting and planning, and Oracle Financial Services Analytic Applications (OFSAA) for market and credit risk analysis. Oracle also offers CCM software that integrates with the GRC platform. Sales growth is solid. Although the platform is often included as part of a broader ERP deployment, many Gartner clients are comparing it in competitive EGRC platform bids. Oracle has shifted back to the Leaders quadrant from the Challengers quadrant, primarily because of better clarity of its GRC strategy and how it fits into the broader Oracle platform.

Strengths

- Market Understanding and Strategy — In evidence of a strong business performance orientation, Oracle promotes the ability to integrate its EGRC platform with Hyperion Financial Manager and Enterprise Performance Management.

- Product Strategy — Oracle has shrewdly recognized that GRC is a collection of discrete activities bound together by a common framework. It employs a "crawl, walk, run" model to effectively position its capabilities to the needs at hand. The more comprehensive a client's approach to GRC, the more capabilities are activated. The long-term vision of improving performance appeals to a top-down buyer looking for a broad set of functionality that can be employed when needed.

- Geographic Strategy — Oracle is a megavendor with global presence and support.

- Product — It has strengths in risk management and policy management. Oracle has good qualitative risk management. Its quantitative risk management includes Monte Carlo simulation, which is available through integration with Oracle Crystal Ball. Oracle has the exceptional ability to map policies to authoritative sources, such as regulations, and to risks and controls. Its data-driven navigation is excellent.

- Market Responsiveness and Track Record — Oracle experienced solid sales performance in 2010 and early 2011. Not surprisingly, many customers are opting for Oracle GRC Suite as part of a larger overall Oracle deal or product strategy. Oracle is also evaluated by non-Oracle application customers.

Cautions

- Product Strategy — Oracle's breadth of offerings is both a blessing and a curse. Customers must be certain which products need to be licensed to support their intended use cases, because real philosophic differences exist among market competitors. This is especially true in the financial services sector, which may need to be supported by an integrated solution of Enterprise GRC Manager, Reveleus and other specialized risk analysis tools.

Gartner.

- Product — Customer references indicated that they need improved integration of the GRC suite with external reporting and office productivity tools. This is surprising, given Oracle's position as a leader in the BI and corporate performance management marketplaces. Some customers do not buy or implement the GRC Intelligence product (part of the GRC Suite) right away, which may contribute to this comment. Obviously, users demand tighter integration, not just best-in-class products.

- Customer Experience — All were satisfied, but many cited areas for improvement at a frequency far higher than other vendors' references. They cited areas for improvement that include reporting, risk content, quantitative risk assessment and audit management.

SAP

SAP offers several GRC-related products as part of the SAP BusinessObjects GRC portfolio. For this evaluation, it demonstrated Process Control/Risk Management for SAP GRC 10, which is currently in ramp-up. With SAP GRC 10, SAP has resolved issues with integration of its core products under its GRC umbrella, and also delivered improved audit management and policy management. Although SAP GRC 10 is still in ramp-up, a process that restricts customer use, the generally available version, Process Control/Risk Management 3.0, which was released last year, has gotten solid market response. Based on the market response during the past year, a strategy that includes GRC-related products that are integrated to provide the applications for risk management and compliance programs, the ability to integrate GRC and performance management, and the ability to integrate the reporting from its CCM tools with the EGRC platform and its strategy, SAP is a highly viable vendor in this market and moves from the Visionaries quadrant to the Leaders quadrant.

Strengths

- Market Understanding and Strategy — SAP has developed a good understanding of the strategic direction of the GRC market. It has aligned its strategy to meet both the basic compliance and risk assessment requirements, and also to the more advanced perspective of the effects of risk management on business performance and decision making.

- Product Strategy — SAP's strategy includes the integration of CCM and a partner strategy to enable a wide array of GRC capabilities. SAP has rearchitected its platform to support better integration of GRC.

- Vertical/Industry Strategy — SAP has specialized solutions for EH&S and trade compliance that can be integrated with its EGRC platform. It is also maintaining a network of partners that provide specialized industry software and content, including partnerships with Deloitte, PwC, Novell, CA, Oversight Systems, Greenlight Technologies and SenSage, among others.

- Innovation — SAP has demonstrated forward thinking through integration of risk management and performance management solutions, and has developed a rearchitected EGRC platform that integrates its core GRC functionality well.

- Geographic Strategy — SAP is a large vendor with global presence and support.

Cautions

- Product Strategy — Customers may have to purchase licenses for multiple core GRC products and partner products to get the advanced functionality like integrated CCM that SAP stresses in its GRC marketing. In addition to its default content, SAP markets the availability of content libraries from PwC and Deloitte; however, these are available only through engagements with those consultancies. Notably, all SAP GRC customer references reported using a third-party consultant during implementation, which can add costs.

- Product — Because it does not support scoping and prioritization of the audit universe well, audit management functionality is not scalable for a large internal audit organization. Also, some of the audit functionality demonstrated required the additional licensing and integration of BI Explorer. Although CCM is not a core capability for an EGRC platform, SAP's Process Control includes CCM for transactions, and customers noted it as not useful for improving auditor productivity.

- Customer Experience — Customers, none of whom were using the GRC 10 version that was demonstrated, noted that improvements were needed in reporting, in audit management and in the CCM feature of Process Control. GRC 10 has improved reporting and integration of audit management, and SAP has engaged Oversight Systems as its primary partner for providing advanced CCM for transactions.

SAS

SAS demonstrated SAS Enterprise GRC version 4.3, which was released in December 2010. SAS is known for strong capabilities in ORM and broad-based risk analytics, with numerous algorithms for predictive and descriptive analytics, including Monte Carlo simulation for robust scenario analysis. Its platform supports compliance and audit functionality well. The company offers a host of complementary GRC-related products and supports diverse functions, such as fraud, sustainability and social media analytics for managing reputational risk.

Strengths

- Market Understanding and Strategy — As the market moves from a compliance focus to a risk and performance orientation, SAS is able to capitalize on its inherent strength and long legacy in this space. The company is known as an analytics, BI and performance management company, with a core emphasis on risk management.

- Product Strategy — SAS's exceptional risk analytics support a large variety of risk management needs through integration with other SAS capabilities. This risk point of view is rippled throughout the product, with solid risk scoping now available for audit management. The company still partners with BPS Resolver for extended audit management capabilities.

- Vertical/Industry Strategy — SAS has targeted banks, insurance firms and electrical utilities. Its operational risk loss database includes publicly reported losses from banks and other industries. SAS also has a library of key performance indicators and key risk indicators for the electrical utilities sector.

- Innovation — The company spends approximately 22% of its annual revenue on R&D, one of the highest reported for this research cycle. SAS also has a lot of GRC-related capabilities that can be integrated in the EGRC platform, including case management, and credit and market risk management.

- Geographic Strategy — SAS is a large vendor with global presence and support, and the product is available in 15 languages.

- Product — SAS has highly advanced capabilities to evaluate a broad spectrum of risks, including risks to strategic business objectives. Visualization of relationships among risks, controls, business objectives, mandates, policies and other entities is exceptional.

Cautions

- Product — Its platform does not adequately support all aspects of policy life cycle management, and IT GRC-specific capabilities are present but were not well-demonstrated. Audit management is satisfactory for a small to midsize audit organization. Until these capabilities are improved, SAS counts on integrating with partners' solutions to meet advanced audit management and policy management needs.

- Market Responsiveness and Track Record — Even though sales growth accelerated in 2010, and the momentum appears to be on the rise, there are still fewer than 125 EGRC customers.

Software AG

Software AG offers the ARIS Solution for GRC. It demonstrated ARIS Risk and Compliance Manager version 3.1, SR 4, and also included ARIS Business Architect 7.1 and ARIS PPM 5.2. Software AG acquired IDS Scheer in 2009. Software AG fully supports a GRC strategy and has injected new momentum. Software AG's road map includes advanced capabilities for a closed-loop process of automated remediation of process risk. Based on an innovative approach to the market with a vision for increasing automation and business process integration, Software AG moves from the Challengers quadrant to the Visionaries quadrant. Despite efforts during the past two years to make improvements, audit management and policy management remain challenges.

Strengths

- Market Understanding and Strategy — Software AG places a heavy emphasis on maximizing the role of business process management in GRC. Its vision is for a fully automated system for identification, monitoring and remediation of risks associated with business processes.

- Product Strategy — Software AG includes ad hoc reporting capabilities via mashups that enable powerful dynamic dashboard configuration capabilities. It is enabling integration with webMethods to support CCM.

- Product — Software AG is very strong on compliance. Modeling capabilities enable a strategic governance-oriented approach to the analysis of risks, controls and business processes.

- Vertical/Industry Strategy — Software AG has developed a broad set of industry-specific content packages.

- Customer Experience — Software AG reference clients indicate that the product functionality often exceeded expectations.

Cautions

- Product Strategy — Improved audit management, which has not been a strong point, is scheduled to be delivered in 3Q11.

- Customer Experience — Reference clients indicate that data collection with ERP and other business applications can be improved.

- Product — Despite a focus on improving policy management, it remains a challenge because of limited content management.

Thomson Reuters

Thomson Reuters demonstrated Enterprise GRC version 4.2, released in October 2010, which is part of the Thomson Reuters Accelus Suite. Thomson Reuters also offers Enterprise GRC in a SaaS version called GRC on Demand, and an audit-management-only version called AutoAudit. The Enterprise GRC platform has all the core functions and has strengths in audit management. Thomson Reuters maintains a large and growing GRC customer base. In 2010, Thomson Reuters acquired Complinet, a GRC vendor that focused on regulatory content services and regulatory change management for the banking and broker-dealer industries. It included Complinet, its legal content service offering Westlaw, EGRC and other GRC-related assets in a new GRC business division, and branded them the Accelus Suite. Notably, some of Thomson Reuters' GRC-related software offerings include TopOffice for credit, risk and ORM for financial services. Some content services for highly regulated industries like financial services and healthcare remain outside the GRC division. Thomson Reuters' move from the Challengers quadrant to the Leaders quadrant reflects its renewed emphasis on the GRC marketplace through the focus brought about by its new GRC division, which is housed in the Thomson Reuters Professional business.

Strengths

- Product Strategy — Thomson Reuters has been very successful with its SaaS delivery model, and also offers a traditional on-site implementation. Thomson Reuters uses its strength as a content provider to differentiate the EGRC platform. It has a strong focus on the legal GRC buyer, who is often looking for regulatory tracking services and regulatory change management supported by good policy management.

- Vertical/Industry Strategy — Thomson Reuters has a wealth of legal, financial, audit and industry-specific content, such as Westlaw and Complinet, that can be integrated with its Enterprise GRC platform. Its road map shows plans for improvements in content services, such as EH&S, and expansion into highly regulated vertical industries.

- Innovation — Thomson Reuters has the highest percentage of revenue invested in R&D of any EGRC platform vendor.

- Geographic Strategy — Thomson Reuters is a global vendor with a direct presence in multiple geographies. EGRC-specific sales and support are focused on North America and Europe, with partnerships in other geographies.

- Product — Thomson Reuters is very strong in audit management and compliance, with reasonable support for risk management. It can provide enhanced quantitative risk management for credit, market and operational risks through integration with Thomson Reuters' TopOffice product.

- Market Responsiveness and Track Record — Thomson Reuters continues to experience strong growth in new customers. It has an optional SaaS delivery mode that is attractive to many companies seeking to minimize upfront costs, especially small and midsize businesses, many of which are just entering the market.

Cautions

- Market Understanding and Strategy — The integration of GRC with business performance is not evident in Thomson Reuters' strategy.

- Product Strategy — Thomson Reuters has developed a more cohesive GRC product strategy, but it needs to focus on ease of integration of its other GRC-related offerings (like TopOffice) that bring enhanced functionality to EGRC. To support its vertical industry strategy, Thomson Reuters needs to expand the Complinet regulatory tracking and change management to additional vertical industries besides banking.

- Product — Customers noted that workflow and regulatory change notification could be improved.

Note 1 Defining the Relationship of Governance, Risk Management and Compliance

"Governance," "risk management" and "compliance" are general terms that can apply to a wide range of products, IT initiatives and business requirements. These three terms have many valid definitions throughout the Gartner client base. These definitions illustrate the relationship of the three terms:

- **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 level of uncertainty. Risks are addressed with a balance of mitigation through the application of controls, transfer through insurance, and avoidance or acceptance through governance mechanisms.

- **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.

Note 2 Top-Down and Bottom-Up Approaches to GRCM

- A top-down approach implies that multiple control categories will be measured and reported, including IT, financial and operational requirements. A top-down approach usually requires less detailed requirements for gathering general computer control data, such as configuration and patch data, but places a premium on higher-level reporting to executives. A top-down approach is more appropriately addressed with EGRC platforms than with IT GRCM.

- A bottom-up approach implies greater detail in IT controls for an IT-centric audience. Many organizations use IT GRCM to organize their vulnerability scan, patch and configuration control data. Traditional IT GRCM tools are more appropriate for IT-specific requirements.

Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor that competes in/serves the defined market. This includes current product/service capabilities, quality, feature sets and skills, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability (Business Unit, Financial, Strategy, Organization): Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support and the overall effectiveness of the sales channel.

Market Responsiveness and Track Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word-of-mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs, and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries, as appropriate for that geography and market.