March 16, 2006

The Forrester Wave™: Governance, Risk, And Compliance Platforms, Q1 2006

by Michael Rasmussen

TECH CHOICES

March 16, 2006

The Forrester Wave™: Governance, Risk, And Compliance Platforms, Q1 2006
Axentis And QUMAS Top Our Product Evaluation

by Michael Rasmussen
with John R. Rymer and Samuel Bright

EXECUTIVE SUMMARY

Faced with mandates for tighter corporate governance and enterprise risk management and barraged by compliance regulations, organizations are adopting platforms that are focused on enterprise governance, risk, and compliance (GRC) management. To assess the state of the GRC platform market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top vendors across 99 criteria. The result: Axentis and QUMAS hit the top of the charts because of their thoroughness in covering the GRC space, while BWise and IBM also fall into the Leader category with platforms that have been used for a variety of GRC purposes. This report includes an interactive vendor comparison tool that provides detailed product evaluations and customizable rankings.

TABLE OF CONTENTS

NOTES & RESOURCES

Forrester conducted evaluations in November 2005 and interviewed 30 vendor and user companies, including: Axentis, BWise, Compliance 360, Hyland Software, IBM, OpenPages, Paisley Consulting, Protiviti, QUMAS, and Stellent.

Related Research Documents
"Trends 2006: Enterprise Risk And Compliance"
December 13, 2005, Trends

"Will The Real Risk And Compliance Vendor Please Step Forward?"
November 28, 2005, Market Overview

"The Forrester Wave™: Enterprise Risk Management Consultants, Q4 2005"
October 28, 2005, Tech Choices

"Seven Habits Of Highly Effective Compliance Programs"
July 12, 2005, Best Practices

FORRESTER®

FROM SILOS OF RISK AND COMPLIANCE TO ENTERPRISE GRC MANAGEMENT

Historically, corporate governance was handled departmentally with no consistent establishment of policies and communication across lines of business. Risk management was buried in finance, and perhaps a few obscure corners of the organization, focused on financial risks and not enterprise or operational risks. And compliance was buried either in the legal department or various parts of operations — approached as a project rather than as a sustained process.

Mandates of stricter corporate governance, increased regulations and a growing risk profile are changing the way organizations are approaching GRC.[1]

Increased Compliance Requirements Add To Risk Complexity

Compliance is one critical area of risk that causes confusion and despair within organizations because it is:

- **Tackled as siloed projects.** Frequently, individuals or departments get bogged down in one area of compliance, such as Sarbanes-Oxley (SOX) or privacy laws, but fail to realize that compliance is a challenge that hits nearly every part of the organization: governance, employment, financial assurance, anti-fraud, information management, intellectual property, environmental, international dealings, competitive practices, product quality/safety, workplace health/safety, and government dealings.[2]

- **Becoming a growing burden.** The pressure on organizations is driving compliance to the top of the priority list. In the US alone, nearly 114,000 new regulations have been introduced since the government started collecting this metric in 1981.[3] Add the international requirements that many organizations have — and the figure becomes oppressive.

- **Leading to greater risks because of fragmentation.** With islands of compliance information captured in scattered documents across the organization, senior management becomes incapable of meeting requirements with dire consequences in its attempt to navigate the organization in today's era of increased accountability.

Defining Your GRC Game Plan

Increased risk and regulatory pressures in a distributed enterprise are propelling organizations to craft consistent game plans for centralizing GRC oversight. There are five goals for this consolidation and resulting convergence:

1. Develop a culture of ethics and control by centralizing corporate governance and communicating policies and procedures.

2. Improve confidence, as well as meet regulatory requirements, in the organization's operational and financial integrity.

3. Maintain accurate and timely risk information with visibility, measurement, control, and sharing of risk across the organization.

4. Accurately measure risk and compliance through a consistent and systematic approach, as opposed to disparate approaches that are reactively managed.

5. Measure risks not only at the system or project level, but also at the business-process, business-unit, and organizationwide levels.

Enterprises Begin Adoption Of Platforms To Address GRC

Organizations are to establish a platform that maintains a system of record for GRC. This enables disparate compliance and governance technologies to combine into a coherent regime for managing GRC across the enterprise.

GRC platforms are specifically aimed at creating a centralized hub of risk and compliance documentation, assessment, analysis, and loss information from every part of the business. Providing the functionality in these four areas requires that solutions in this product category have excellent content management, business process management, and workflow capabilities. Solutions in this space must have core features in four areas:

- **Policy, procedure, and control documentation.** These features allow for the development, documentation, and communication of policies, procedures, and controls to the business environment.

- **Risk and control assessment.** These features manage and survey various areas of the business to assess risk, compliance, and controls in the environment.

- **Risk analytics.** These features use the mandates laid forth in policy and control documentation combined with data gathered in risk and control assessments to quantify and model risk to the business.

- **Loss, event, and investigations management.** These features collect records for tracking organization losses, events, gaps in controls, and audit findings while facilitating the investigation and response process.

GRC PLATFORMS EVALUATION OVERVIEW

To assess the state of the GRC platform market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top GRC platform vendors.

Evaluation Criteria

After examining past research, user need assessments, and vendor and expert interviews, Forrester developed a comprehensive set of evaluation criteria (see Figure 1). Forrester evaluated vendors against approximately 99 criteria, which we grouped into three high-level buckets:

- **Current offering.** The focus fell predominantly on four capability areas of a GRC platform: policy, procedure, and control documentation and communication; risk and control assessment; risk analytics; and loss, event, and investigations management. Further consideration and weighting was then given to the vendor features for business functionality; workflow, content, and document management; dashboard, reporting, and monitoring; technology; and client reference experiences and testimonials.

- **Strategy.** The strategy category measured the vendors' product strategy and vision, technology strategy and vision, commitment to research and development, and the breadth of strategic alliances and partnerships.

- **Market presence.** The market presence category measured the vendors' financial viability, current installed base, as well as their sales and delivery footprint in the market.

Evaluation Methodology

Forrester used a combination of 10 vendor surveys and product demos, as well as 20 customer reference calls to assess the strengths and weaknesses of each solution:

- **Vendor surveys.** Forrester surveyed vendors on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed vendor surveys, we conducted vendor calls where necessary to gather details of vendor qualifications.

- **Product demos.** We asked vendors to conduct demonstrations of their product's functionality. We used findings from these product demos to validate details of each vendor's product capabilities.

- **Customer reference calls.** To validate product and vendor qualifications, Forrester also conducted reference calls with two of each vendor's current customers.

Figure 1 Evaluation Criteria

CURRENT OFFERING

Documentation — policies, procedures, and control	How does the platform facilitate the development, documentation, and communication of enterprisewide policies, procedures, and controls?
Assessment — risk, control, and compliance	How does the platform provide for assessing risk and compliance through repeatable and collaborative assessment processes?
Risk analytics	How does the platform measure, model, and visualize corporate risks?
Loss event/incident management	How does the vendor provide a system of record to document organizational losses as well as offer a platform for ongoing investigations management?
Business functionality	What are the platform's capabilities for modeling the business environment and providing a framework for risk and compliance set within a business context?
Workflow, content, and document management	What are the workflow, content, and document management capabilities of the GRC solution?
Dashboard, reporting, and monitoring	What are the dashboard, reporting, and monitoring capabilities of the GRC solution?
Technology	What are the technology capabilities of the GRC solution?
Client interviews	How do the vendor's clients score the platform's GRC capabilities?

STRATEGY

Product strategy and vision	How does the vendor articulate its product strategy and vision for the GRC space?
Technology strategy and vision	What is the vendor's technology strategy and vision?
R&D	How devoted is the vendor to R&D to enhance its GRC capabilities?
Strategic alliances	What strategic alliances are in place that strengthen the vendor's GRC platform and its capabilities?

MARKET PRESENCE

Financial viability	What is the vendor's financial viability?
Installed base	What is the installed base of the vendor's GRC platform?
Delivery footprint	What is the delivery footprint of the vendor's GRC platform?

Source: Forrester Research, Inc.

Evaluated Vendors

Forrester included 10 vendors in the assessment: Axentis, BWise, Compliance 360, Hyland Software, IBM, OpenPages, Paisley Consulting, Protiviti, QUMAS, and Stellent. Each of these vendors has:

- **Features spanning the four capability areas.** Vendors had to be able to support the breadth of a GRC platform: policy, procedure, and control documentation and communication; risk and control assessment; risk analytics; and loss, event and investigations management.

- **Clients using the platform for more than one GRC purpose.** In total, Forrester estimates that there are more than 40 vendors that have features covering the four defined feature areas — however, many of these platforms are being used for only one GRC area (e.g., SOX, health and safety). Vendors were selected based on their ability to provide references spanning the spectrum of GRC purposes.

- **Established and recognized market presence.** Finally, vendors were selected based on the volume of inquiry questions about them from Forrester clients.

LEADERS HAVE DEPTH OR BREADTH IN UNDERSTANDING GRC

The evaluation uncovered a market in which (see Figure 2):

- **Axentis, BWise, IBM, and QUMAS lead the pack.** Breadth and depth defines a Leader in this market. Each of these vendors made it to the leader category by demonstrating that their platforms are being used for a range of GRC purposes. QUMAS is specifically focused on financial services and life sciences organizations — and showed an amazing understanding and applicability of its platform for GRC in these verticals. Axentis was the only platform solely focused on software as a service and showed the broadest use of its platform for GRC purposes. BWise and IBM demonstrated that they have the right capabilities with clients using their platforms for more than one GRC purpose.

- **Paisley, Protiviti, OpenPages, and Stellent offer competitive options.** These vendors have very capable and competitive offerings — in fact, they have all of the right features to make them leaders except for the fact that they are largely deployed for a single GRC purpose: SOX. Protiviti, while a capable product, was hurt by its client reference feedback illustrating difficulties in a professional services firm moonlighting as a software vendor.

- **Compliance 360 and Hyland Software fall short.** Both Compliance 360 and Hyland Software have strengths, but they fell behind in the specific feature functionality of their current offerings. Hyland Software has the right components under the hood, but its answers and demonstration

showed that this requires more custom development/work than the purpose-built solutions that the leading platforms provided. Compliance 360 showed its strength in regulatory intelligence and management but did not have the broad features of the Leaders.

This evaluation of the GRC market is intended only as a starting point. Readers are encouraged to view detailed product evaluations and adapt the criteria weighting to fit their individual needs through the Forrester Wave Excel-based vendor comparison tool.

Figure 2 Forrester Wave™: Governance, Risk, And Compliance Platforms, Q1 '06

Source: Forrester Research, Inc.

Figure 2 Forrester Wave™: Governance, Risk, And Compliance Platforms, Q1 '06 (Cont.)

	Forrester's Weighting	Axentis	BWise	Compliance 360	Hyland Sotware	IBM
CURRENT OFFERING	50%	4.29	3.85	1.58	2.31	3.19
Documentation — policies, procedures, and control	20%	4.70	3.50	1.80	2.10	3.20
Assessment — risk, control, and compliance	20%	4.80	4.40	1.00	2.30	3.20
Risk analytics	15%	3.00	3.70	0.00	1.00	2.80
Loss event/incident management	15%	4.10	3.70	2.10	1.60	2.00
Business functionality	5%	4.30	3.50	1.00	2.00	4.10
Workflow, content, and document management	5%	3.90	3.90	1.60	4.60	4.20
Dashboard, reporting, and monitoring	5%	4.20	3.40	1.00	2.30	4.10
Technology	5%	5.00	4.60	1.70	4.20	5.00
Client interviews	10%	4.59	3.88	4.43	3.87	3.25
STRATEGY	50%	4.48	3.44	2.32	2.32	4.12
Product strategy and vision	40%	4.20	3.60	1.40	2.40	2.80
Technology strategy and vision	20%	5.00	3.00	1.00	1.00	5.00
R&D	30%	5.00	3.00	5.00	3.00	5.00
Strategic alliances	10%	3.00	5.00	0.60	2.60	5.00
MARKET PRESENCE	0%	3.10	4.00	1.50	2.85	3.40
Financial viability	25%	3.00	3.00	3.00	5.00	5.00
Installed base	50%	3.20	4.00	1.00	1.20	1.80
Delivery footprint	25%	3.00	5.00	1.00	4.00	5.00

All scores are based on a scale of 0 (weak) to 5 (strong).

Source: Forrester Research, Inc.

Figure 2 Forrester Wave™: Governance, Risk, And Compliance Platforms, Q1 '06 (Cont.)

	Forrester's Weighting	OpenPages	Paisely Consulting	Protiviti	QUMAS	Stellent
CURRENT OFFERING	50%	3.25	2.90	2.81	4.40	3.38
Documentation — policies, procedures, and control	20%	3.00	3.00	2.60	4.70	3.50
Assessment — risk, control, and compliance	20%	3.00	3.10	3.00	4.80	3.00
Risk analytics	15%	2.90	2.90	2.40	3.20	2.40
Loss event/incident management	15%	2.90	2.15	2.75	4.70	2.90
Business functionality	5%	3.20	3.00	3.40	4.10	3.60
Workflow, content, and document management	5%	3.80	2.65	2.80	4.30	5.00
Dashboard, reporting, and monitoring	5%	4.20	3.00	3.00	3.50	3.50
Technology	5%	3.90	2.60	2.80	5.00	5.00
Client interviews	10%	4.20	3.64	3.17	4.65	4.30
STRATEGY	50%	3.80	2.80	2.80	4.52	3.20
Product strategy and vision	40%	3.00	2.60	2.60	4.80	3.00
Technology strategy and vision	20%	3.00	3.00	3.00	3.00	3.00
R&D	30%	5.00	3.00	3.00	5.00	3.00
Strategic alliances	10%	5.00	2.60	2.60	5.00	5.00
MARKET PRESENCE	0%	2.50	2.45	3.70	2.90	3.80
Financial viability	25%	3.00	3.00	5.00	3.00	5.00
Installed base	50%	2.00	2.40	2.40	2.80	2.60
Delivery footprint	25%	3.00	2.00	5.00	3.00	5.00

All scores are based on a scale of 0 (weak) to 5 (strong).

Source: Forrester Research, Inc.

VENDOR PROFILES

Leaders

- **QUMAS QCompliance Suite.** QUMAS has thought leadership and a strong feature set that distinguishes it as a Leader in GRC platforms. The QCompliance Suite is a mature offering that has been used in complex risk and compliance environments for 12 years. Furthermore, QUMAS was one of the few vendors in our Wave evaluation with reference implementations for a range of risk and compliance purposes in large enterprises, as opposed to single-purpose implementations. The QCompliance Suite is strong across the board, with particular strengths as a GRC platform in life sciences and financial services. In these respective verticals, QUMAS pulled ahead of the competition by demonstrating a detailed understanding of risk and compliance — and strong references.[4]

- **Axentis Enterprise (Ae).** Axentis rose to be a GRC Leader by demonstrating the broadest use of its platform among the vendors compared in our Wave evaluation. The vendor has more installed seats than any other GRC platform vendor, as well as the widest range of risk and compliance applications. Axentis Enterprise is available as a subscription service, providing further distinctive differentiation among its competitors.[5]

- **BWise.** BWise established itself as a Leader in the GRC platform market through its ability to manage and monitor enterprise and operational risks. The BWise platform is used for a variety of risk and compliance purposes; however, risk management is where it differentiates itself from the rest. The platform is particularly strong in identifying and tracking key business risk and performance indicators.[6]

- **IBM Workplace for Business Controls and Reporting.** IBM established its Workplace for Business Controls and Reporting (WBCR) as a leader in the GRC platform space by demonstrating its abilities to openly integrate into the broader technology architecture of an organization. Customers can augment WBCR with IBM's systems-integration capabilities and a range of other IBM solutions to meet GRC requirements. The WBCR platform can manage a range of risk and compliance requirements, but to date, has predominantly been deployed in response to SOX.[7]

Strong Performers

- **OpenPages GRCM.** OpenPages, with its OPtimum Governance Risk and Compliance Management (GRCM) suite, is a Strong Performer in the GRC platform market. For the past two years, customer implementations of the product have been focused on SOX, but OpenPages is ready to tackle broader enterprise GRC requirements as well. The current release supports operational risk management, and the company plans future modules to manage IT risk and financial controls management. This release recently shipped and customers had yet to go live on the platform, thus preventing OpenPages from being considered a Leader in this Wave evaluation. The OpenPages suite differentiates itself on the development and management of key risk indicators (KRI), particularly through its partnership with Risk Business and its KRI framework.[8]

- **Stellent Universal Content Management.** With its Universal Content Management platform, Stellent leverages its experience in content management to provide a solution that can be tailored to meet specific GRC purposes. Whereas some content management players have generically approached GRC requirements, Stellent has built a specific application to meet GRC requirements. Stellent has predominantly focused its GRC marketing efforts on SOX, but clients use its platform for a broad range of GRC purposes. The Stellent platform provides a solution to organizations that want to leverage the platform for broader content management investments as well as for GRC purposes.[9]

• **The Paisley Solution.** With its Risk Navigator platform, Paisley Consulting has developed a strong reputation in the SOX market in the past few years. While predominantly adopted for SOX compliance, Risk Navigator is applicable to broad GRC management. The unique strength of the Risk Navigator platform is the direct support and integration of auditors and audit processes into GRC management and oversight.[10]

• **Protiviti Governance Portal.** The Protiviti Governance Portal (PGP) is a Strong Performer in the GRC platform market. The particular strength that sets the PGP solution apart is the depth and experience that Protiviti has in GRC consulting — providing a one-stop shop for consulting and GRC software. Protiviti's history in GRC consulting is also evident in the rich risk taxonomy and management content of the product.[11]

Contenders

• **Hyland Software OnBase.** OnBase from Hyland Software provides a content management and workflow platform that can be architected for GRC purposes. While the platform does not have deep GRC content, it does provide a solid foundation in its array of content management features and enables organizations to leverage the platform for other content management requirements.[12]

• **Compliance 360.** Compliance 360 provides a compliance platform that is particularly adept at regulatory intelligence. Through content relationships with providers such as LexisNexis, the Compliance 360 platform helps gather and disseminate regulatory information within the enterprise. While not focused on the risk aspects of GRC, the Compliance 360 platform provides a capable compliance management solution, particularly for those in the healthcare and insurance verticals.[13]

SUPPLEMENTAL MATERIAL

Online Resource

The online version of Figure 2 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings.

The Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria to be evaluated in this market. From that initial pool of vendors, we then narrow our final list. We choose these vendors based on: 1) product fit; 2) customer success; and 3) Forrester client demand. We eliminate vendors that have limited customer references and products that don't fit the scope of our evaluation.

After examining past research, user need assessments, and vendor and expert interviews, we develop the initial evaluation criteria. To evaluate the vendors and their products against our set of criteria, we gather details of product qualifications through a combination of lab evaluations, questionnaires, demos, and/or discussions with client references. We send evaluations to the vendors for their review, and we adjust the evaluations to provide the most accurate view of vendor offerings and strategies.

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in the Forrester Wave document — and then score the vendors based on a clearly defined scale. These default weightings are intended only as a starting point, and readers are encouraged to adapt the weighting to fit their individual needs through the Excel-based tool. The final scores generate the graphical depiction of the market based on current offering, strategy, and market presence. Forrester intends to update vendor evaluations regularly as product capabilities and vendor strategies evolve.

ENDNOTES

[1] Organizations face many risks: strategic, financial, litigation/legal, product/services, operational, environmental, health and safety, geopolitical, suppliers, business partners, technology, workforce, project, compliance, and reputation. The list of risks appears endless.

[2] The identified areas of compliance in this report come from the taxonomy that has been built from the Open Compliance and Ethics Group (OCEG). OCEG is showing thought leadership in providing a consistent framework to manage compliance across the organization. Source: Open Compliance and Ethics Group (http://www.oceg.org/).

[3] The US Office of Information and Regulatory Affairs (part of the Office of Management and Budget) reports annually to Congress on trends in federal regulatory activity. "Since OMB began to compile records in 1981, Federal agencies have published 113,798 final rules in the Federal Register. Of these final rules, 20,393 were reviewed by OMB under Executive Order procedures. Of these OMB-reviewed rules, 1,119 were considered 'major' rules, primarily due to their anticipated impact on the economy (e.g., estimated

costs and/or benefits were in excess of $100 million annually). To the best of OMB's knowledge, most of these rules have never been subject to an 'ex post' analysis to determine whether they worked as intended and what their actual benefits and costs were. There is no systematic and comprehensive requirement for federal agencies to validate their pre-regulation estimates of benefits and costs based on actual experience with the rule." Source: Draft 2005 Report To Congress On The Costs And Benefits Of Federal Regulations (http://www.whitehouse.gov/omb/inforeg/2005_cb/draft_2005_cb_report.pdf).

[4] For more detailed analysis on how QUMAS fared in this evaluation, view the QUMAS summary. See the March 16, 2006, Tech Choices "QUMAS Is A Leader In Governance, Risk, And Compliance Platforms."

[5] For more detailed analysis on how Axentis fared in this evaluation, view the Axentis summary. See the March 16, 2006, Tech Choices "Axentis Is A Leader In Governance, Risk, And Compliance Platforms."

[6] For more detailed analysis on how BWise fared in this evaluation, view the BWise summary. See the March 16, 2006, Tech Choices "BWise Is A Leader In Governance, Risk, And Compliance Platforms."

[7] For more detailed analysis on how IBM fared in this evaluation, view the IBM summary. See the March 16, 2006, Tech Choices "IBM Is A Leader In Governance, Risk, And Compliance Platforms."

[8] For more detailed analysis on how OpenPages fared in this evaluation, view the OpenPages summary. See the March 16, 2006, Tech Choices "OpenPages Is A Strong Performer In Governance, Risk, And Compliance Platforms."

[9] For more detailed analysis on how Stellent fared in this evaluation, view the Stellent summary. See the March 16, 2006, Tech Choices "Stellent Is A Strong Performer In Governance, Risk, And Compliance Platforms."

[10] For more detailed analysis on how Paisley Consulting fared in this evaluation, view the Paisley Consulting summary. See the March 16, 2006, Tech Choices "Paisley Consulting Is A Strong Performer In Governance, Risk, And Compliance Platforms."

[11] For more detailed analysis on how Protiviti fared in this evaluation, view the Protiviti summary. See the March 16, 2006, Tech Choices "Protiviti Is A Strong Performer In Governance, Risk, And Compliance Platforms."

[12] For more detailed analysis on how Hyland Software fared in this evaluation, view the Hyland Software summary. See the March 16, 2006, Tech Choices "Hyland Software Is A Contender In Governance, Risk, And Compliance Platforms."

[13] For more detailed analysis on how Compliance 360 fared in this evaluation, view the Compliance 360 summary. See the March 16, 2006, Tech Choices "Compliance 360 Is A Contender In Governance, Risk, And Compliance Platforms."

FORRESTER®

Helping Business Thrive On Technology Change

Headquarters

Forrester Research, Inc.

400 Technology Square

Cambridge, MA 02139 USA

Tel: +1 617/613-6000

Fax: +1 617/613-5000

Email: forrester@forrester.com

Nasdaq symbol: FORR

www.forrester.com

Research and Sales Offices

Australia	Israel
Brazil	Japan
Canada	Korea
Denmark	The Netherlands
France	Switzerland
Germany	United Kingdom
Hong Kong	United States
India	

For a complete list of worldwide locations, visit www.forrester.com/about.

For information on hard-copy or electronic reprints, please contact the Client Resource Center at +1 866/367-7378, +1 617/617-5730, or resourcecenter@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research (Nasdaq: FORR) is an independent technology and market research company that provides pragmatic and forward-thinking advice about technology's impact on business and consumers. For 22 years, Forrester has been a thought leader and trusted advisor, helping global clients lead in their markets through its research, consulting, events, and peer-to-peer executive programs. For more information, visit www.forrester.com.

FORRESTER®