

August 7, 2006

Overcoming Risk And Compliance Myopia

by Michael Rasmussen

MARKET OVERVIEW

MARKET OVERVIEW



August 7, 2006

Overcoming Risk And Compliance Myopia

GRC Software Platform Market Landscape

This is the second document in the "Risk And Compliance Market Landscape" series.

by **Michael Rasmussen**

with Laura Koetzle, Sarah Bernhardt, and Lauren Sessions

EXECUTIVE SUMMARY

Organizations confront a complex web of compliance mandates and enterprise risks. Historically, they have treated their risks and compliance initiatives as independent silos that they scatter across distributed business operations around the globe. With increased focus on corporate governance and enterprise risk management, firms need governance, risk, and compliance (GRC) software platforms to drive sustainability, efficiency, and consistency in managing enterprise risk and compliance. The GRC software platform market has grown from \$85 million in 2002 to \$590 million today, and Forrester projects that it will expand to \$1.3 billion by 2011. Today, the GRC software platform market is fragmented and includes 64 vendors — thus, it's ripe both for further specialization of products and consolidation of small vendors.

TABLE OF CONTENTS

- 2 **Organizations Struggle With Risk And Compliance**
- 3 **Getting Glasses: How The GRC Software Platform Helps Firms Regain Control**
- 9 **The Technical Support That GRC Software Platforms Need To Succeed**
- 10 **Making Sense Of A Fragmented GRC Software Platform Market**
- 16 **GRC Software Platforms: The Next Five Years**

RECOMMENDATIONS

- 18 **Define Your Risk And Compliance Architecture**

ALTERNATIVE VIEW

- 19 **Growth Continues To Skyrocket If GRC Expands To Business Performance**
- 20 **Supplemental Material**

NOTES & RESOURCES

Forrester interviewed 64 vendors for this report.

Related Research Documents

["The Forrester Wave™: Governance, Risk, And Compliance Platforms, Q1 2006"](#)

March 16, 2006, Tech Choices

["Sarbanes-Oxley Compliance Software 2006: Momentum Will Shift To Controls Optimization"](#)

March 9, 2006, Market Overview

["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

["Seven Habits Of Highly Effective Compliance Programs"](#)

July 12, 2005, Best Practices

TARGET AUDIENCE

Security and risk professional

ORGANIZATIONS STRUGGLE WITH RISK AND COMPLIANCE

Responsibility for risk and compliance has traditionally been scattered across legal, finance, IT, and business operations. Faced with multiple risk and compliance initiatives scattered across business operations, the burden of risk and compliance has become a widespread business problem. In some industries, such as pharmaceuticals, regulations and the complex nature of risk weigh heavily on nearly every aspect of the business.¹ These challenges are driving organizations to look for new approaches to GRC management. Consider the following:

- **Business complexity introduces greater risk.** Firms have been re-engineered and outsourced to the point that it becomes difficult to discern organizational boundaries. These organizations operate globally to reduce the cost of operations and seek advantage in new markets. However, operating in diverse geographic and legal jurisdictions increases exposure to political instability, terrorism, and environmental risks, and introduces varying or even conflicting regulatory compliance requirements from a range of jurisdictions.² Complexity of business operations requires an organization to stay on top of a dynamic risk environment — a slight mishap can have grave effects on an organization's reputation, integrity, operations, and relationships. Miscalculating politics in differing regions of the globe can close markets or hinder the organization from seizing new opportunities at the right time.
- **Multiplying regulations complicate compliance.** Regulations are streaming out of governments nonstop — since 1981, the US federal government alone has introduced 114,000 new rules and regulations that affect business.³ In fact, the Cato Institute reported in 2004 that the regulatory impact on the US economy alone was approaching \$1 trillion annually.⁴ Two years later, Forrester estimates that the US has now passed the \$1 trillion total economic impact from compliance. Because each distinct legal jurisdiction in which a global firm operates may impose an equally enormous set of regulatory burdens, that firm's compliance cost skyrockets. Thus, organizations need a taxonomy that identifies the best practices for achieving global compliance.⁵
- **Failure to relate risk and compliance can retard governance improvements.** Risk and compliance are not disconnected islands — they are two sides of the same coin. Organizations that fail to identify compliance as part of their enterprise risk management program are bound for a trail of business mishaps and wrong turns. Litigation, negative publicity, compliance failures, poor business execution, and lapse of corporate ethics all combine to negatively affect the firm and weaken its corporate governance. Furthermore, government prosecutors are becoming increasingly aggressive in combating fraud and ethical wrongdoing. From Enron to

Elliot Spitzer, government is stepping up to the role of holding organizations accountable for mishaps.

Historically, Organizations Approached Risk And Compliance Myopically

Risk and compliance processes burden line-of-business executives with repeated assessments that ask the same questions for different risk and compliance purposes. Organizations that fail to take an enterprise approach to risk and compliance end up with duplicate technologies and inconsistent approaches, measurement, and reporting — resulting in islands of information scattered throughout the enterprise. Meaning? Most organizations suffer from risk and compliance myopia. For example:

- **Unknowingly, an insurer had four different projects to evaluate risk and compliance tools.** The insurance company's IT executives wanted to know which consultants and software solutions could help them manage risk and compliance. Forrester interviewed IT and varying business departments and discovered four projects already in flight: two in the IT group, one under the CFO, and one in the compliance department. Each was conducting a review of available technology to manage risk and compliance based on similar requirements, and each had chosen a different technology direction.
- **Stovepipes of risk and compliance drove one bank to evaluate GRC technology.** A major bank engaged Forrester to assess its risk and compliance processes and how technology could create efficiencies and consistency into its enterprise risk management (ERM) program. The bank has a large ERM group with a chief risk officer (CRO) and includes compliance in its ERM program. Forrester discovered that despite its ERM organization's lofty goals, the firm still tackled risk and compliance in stovepipes, trapping information in silos of paper and electronic documents. Dishearteningly, the lines of business still saw risk and compliance activities as pure cost.

GETTING GLASSES: HOW THE GRC SOFTWARE PLATFORM HELPS FIRMS REGAIN CONTROL

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 an octopus-like challenge.⁶ Managing this many-tentacled beast requires that an organization establish a technology architecture for GRC.

What Is The Value Of The GRC Software Platform?

The GRC software platform enables an enterprise risk and compliance strategy; the software itself is *not* a strategy. To get the most value out of a GRC software platform requires that existing risk and compliance organizational structure and processes are in place that the software can support and enhance through technology enablement. GRC software platforms must be:

- **Sustainable.** Although firms might wish otherwise, risk and compliance activities are not going away. Organizations that have approached risk and compliance as a project have learned the hard way that it needs to be managed as a process. The dynamism of business results in rapid changes to business processes, relationships, and technologies that firms must continually map to risk and compliance requirements. When firms add new acquisitions, relationships, lines of business, or products, compliance officers must keep abreast of changes. The only way to build a sustainable risk and compliance process is to invest in a GRC software platform.
- **Consistent.** In an era of increased accountability and corporate governance, firms can't afford not to consistently understand, approach, and measure risks and controls. The GRC software platform provides a centralized hub with which to manage risk and compliance across a firm's disparate business silos. Using business process and content management technologies, GRC software can maintain a consistent taxonomy, approach, and accuracy of risk- and control-related information and communication. GRC software platforms allow an organization to centrally store policies, procedures, and controls as well as use common assessment processes, and then information that is gathered can be reused for other assessments.
- **Efficient.** Business operations today struggle with risk and compliance processes that have been stovepiped, ad hoc, and inconsistent. Gathering risk information once, as opposed to through a barrage of independent assessments asking the same questions, alleviates the frustration of line-of-business organizations. GRC software platforms automate risk and compliance processes with workflow, content management, and collaboration features, thus relieving the burden on the business through the shared use of information across assessments instead of taxing the business by asking them the same question week after week.

What's A GRC Software Platform, And What Does It Do?

The GRC software platform is the technology heart of the GRC architecture: It provides a single system of record for defining, maintaining, and monitoring governance, risk, and compliance. A GRC software platform is also the “heart” that connects complex risk and compliance processes across the organization. GRC platforms create centralized systems of record for the entire business in four areas (see Figure 1):

1. **Policy, procedure, and control documentation, maintenance, and communication.** Policies and controls are central to operational risk and compliance. The first thing a regulator or auditor wants to see is how the organization has defined its adherence to external requirements. For example, an auditor will want to see how you interpreted SOX 404 controls and applied them to your financial and accounting processes. GRC software platforms provide capabilities specifically built to support the development, maintenance, and communication of policies, procedures, and controls across the organization (see Figure 2).
2. **Risk and control assessment processes.** Documentation and communication of policies and controls mean nothing if the controls are not in place and functioning — this requires workflow

and collection capabilities to assess the state of controls. GRC software platforms support the gathering of information for the assessment process of risk, controls, and compliance. Assessment functionality allows the organization the ability to manage control evaluation not just for a single purpose like SOX but for other compliance purposes as well (see Figure 3).

3. **Risk analytics, modeling, and reporting.** Next, organizations need to analyze and report on the state of risk and controls. This allows executives, business managers, auditors, and regulators to assess the state of risk and compliance. If an executive has a question about the state of risk around supply chain and logistic operations, they can use the system to view the aggregate measure of controls and incidents surrounding these processes. GRC software platforms have risk modeling, charting, graphing, and dashboarding capabilities to visualize and measure risk and compliance across the organization (see Figure 4).
4. **Loss, event collection, and investigations management.** History repeats itself, whether as tragedy or farce, because unaided institutional memories are extremely short. To mitigate future mishaps, organizations must centrally manage investigations and aggregate corporate loss and event information. GRC platforms manage the business process of investigations and collect loss/event metrics across lines of business and corporate processes. The loss functionality allows managers to monitor the losses around and then assign appropriate and cost-effective controls to mitigate future losses (see Figure 5).

Figure 1 Risk And Compliance Market Landscape

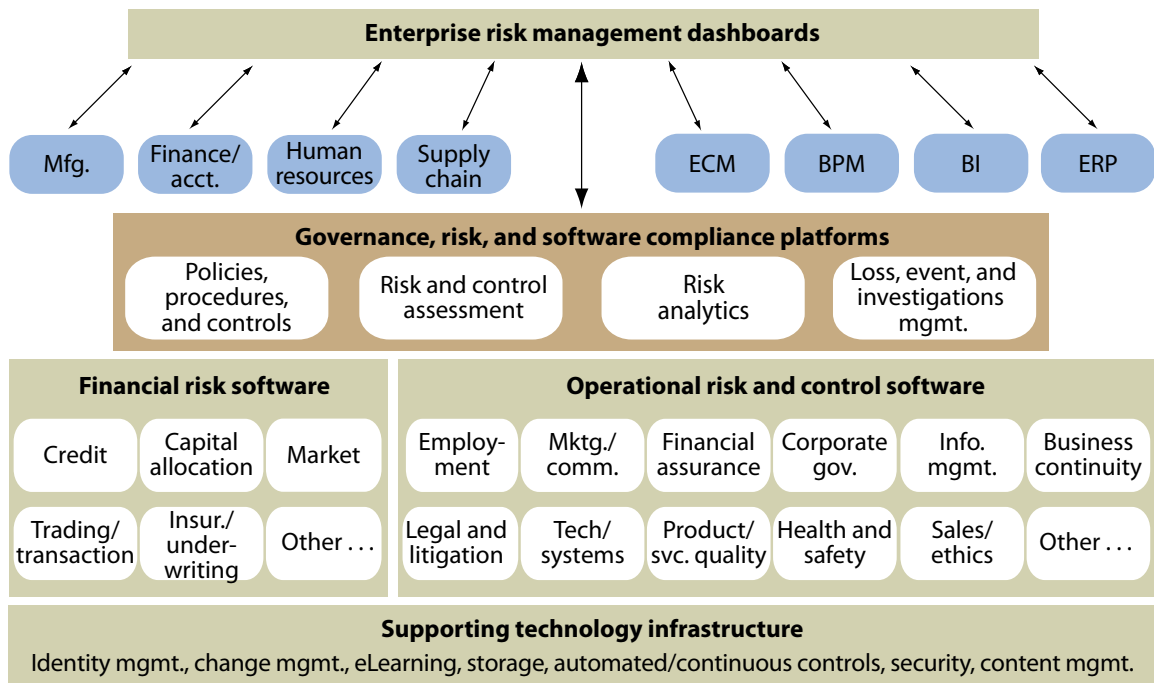


Figure 2 GRC Software Platform Features: Policy And Control Management

Feature	Definition
Definition	Collaborative definition and approval of policies, procedures, and controls throughout the business environment
Maintenance	Ability to periodically manage and automate the review and maintenance of corporate policies and controls
Communication	Capability for an individual to log into the system and see all of the policies, procedures, and controls that apply to his or her role and responsibility in the organization
Acceptance tracking	Tracking employee and business partner acknowledgement and commitment to adhering to policies
Training and awareness	Content features to push training and awareness, eLearning, and testing to validate employee and stakeholder understanding of policies and controls
Mapping processes and organization	Features to map organization business processes and structure to the policy and control environment
Risk and control architectures	Modeling of the control environment around industry-standard risk and control architectures and frameworks
Regulatory and risk intelligence	Capabilities to monitor and feed developments into a process to review new or changing regulations, court rulings, geopolitical risk factors, and enable a review process to identify necessary policy and control changes

40037

Source: Forrester Research, Inc.

Figure 3 GRC Software Platform Features: Risk And Control Assessment Features

Feature	Definition
Scheduling	Ability to schedule and track risk and control assessments
Reuse of information	Features that support the reuse of information already gathered through previous assessment to relieve the burden on the business
Communication	Capability to notify individuals when they have assessment tasks
Workflow and process management	Defined abilities to manage the status and progress of assessments
Business rules	Automation of control status information and enforcement directly into IT systems and business processes
Audit management	Direct links into audit management systems to support the role of audit and audit findings within the system

40037

Source: Forrester Research, Inc.

Figure 4 GRC Software Platform Features: Risk Analytics, Modeling, And Reporting

Feature	Definition
Risk analytics	Integration of a math engine that supports advanced risk analytics (e.g., Monte Carlo, Value at Risk)
Dashboarding	Visualization capabilities to model risk (e.g., heat charts, graphing) and the status of compliance controls
Reporting	Ability to report on risk at multiple levels of the organization — drill up and drill down from the entire business down to individual processes
Performance management	Capabilities to identify and manage key risk indicators and map them over to key performance indicators for the business

40037

Source: Forrester Research, Inc.

Figure 5 GRC Software Platform Features: Loss, Event Collection, And Investigations Management

Feature	Definition
Loss metrics	Definition and reporting on aggregated losses across the organization
Investigations management	Defined workflow and content capabilities to manage and report on investigations and litigation across the organization
Control gaps/audit findings	Ability to track and monitor the status of recognized control gaps and audit findings
Regulatory management	Features to support the documentation of regulator interactions and examinations
Whistleblower	Integration or support of whistleblower capabilities to report and respond to corporate wrongdoing
External loss data	Connection to external loss data for further analysis and comparison and to meet regulatory requirements (e.g., Basel II)

40037

Source: Forrester Research, Inc.

Who Uses A GRC Software Platform?

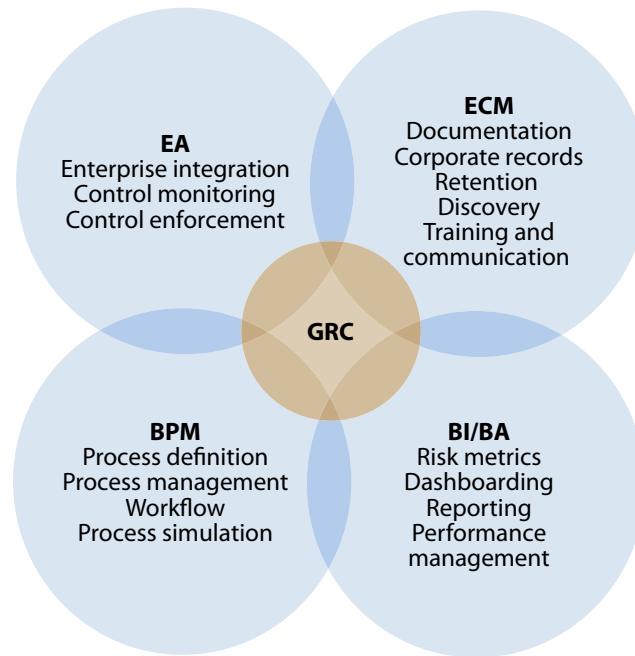
Everyone — really. The GRC software platform manages internal compliance to corporate governance policies and practices, handles external compliance to regulatory and legal requirements, and provides a system for communicating and measuring risk across the enterprise. To succeed in these objectives, every individual — executive, business manager, process owner, employee, contractor, consultant, business partner, and temporary worker — needs access to the system. Usage varies across:

- **Business executives.** Executives use the software to monitor the state of risk and compliance, as well as monitor corporate losses, driving strategic decisions and management of the

organization. They are most interested in the dashboard, reporting, and analytics capabilities. Executives want the ability to understand the aggregate risk and potential impact on business performance.

- **Risk and compliance officers/managers.** Typically, these officers are the heaviest users of the software, because they focus on the day-to-day management of risk and compliance content and processes. Business process management is critical to risk and compliance managers because compliance, to be successful, needs to be integrated within processes. Risk and compliance managers need a system with which they may define a consistent framework of risks and controls, and build processes to manage and monitor them, centrally and on an ongoing basis. For example, risk and compliance managers at commercial banks want a platform to monitor and manage areas of operational risk such as sales practices, international transactions, fraud, and information security in response to Basel II's operational risk requirements.
- **Business unit and process managers.** These executives must use the software to answer risk and control assessments and to monitor the state of risk and compliance for individual areas of responsibility such as sales practices or complying with global trade regulations. As the ultimate owners of risk and controls, the workflow, content, and ERP integration are critical components driving the success of the GRC software platform for business unit and process managers. Business unit and process managers will want to peer into specific areas of risk and compliance pertaining to their roles — factory floor managers need reports on product quality and worker safety.
- **Employees, contractors, consultants, and temporary workers.** The system helps every member of the firm read, acknowledge, and receive training on the policies and compliance issues that pertain to their jobs. This is why GRC platforms need strong content publishing, training/eLearning, and testing capabilities. For example, pharmaceutical field sales reps will sign on to the system and see all the policies, practices, and controls that apply to them. They will go through eLearning modules that train on specifics about compliance with sales and pricing practices mandated for the pharma industry, and they'll use the system to formally assert understanding of corporate sales practices and legal requirements.
- **Business partners.** Business partners (e.g., suppliers, contractors, and outsourcers) work with the system in conducting contract and control assessments to attest to their performance to contractual requirements. Offshore outsourcing firms conduct risk and control self-assessments annually to show their adherence to the process and technical control requirements defined in their contracts with clients. Firms may require business partner employees to acknowledge their understanding and acceptance of policies that govern their use of your company's information and processes, including conformance to privacy and security policies, plus proper ethics and communication practices for call centers.

Figure 6 GRC Software Platforms: Four Technology Areas



40037

Source: Forrester Research, Inc.

THE TECHNICAL SUPPORT THAT GRC SOFTWARE PLATFORMS NEED TO SUCCEED

Achieving integration of the four capability areas that Forrester considers essential for GRC software platforms — policies/controls, assessment, analytics, and loss/investigations — requires that the platforms demonstrate four integrated areas of functionality (see Figure 6):

1. **Enterprise content management.** GRC starts as a content problem. As organizations struggle to manage an assortment of risk assessment and compliance examination documentation, they first look for content management products with which to categorize, store, retain, and manage access to this sensitive information.
2. **Business process management.** After gaining control of content, firms must then drive efficiency with process management and workflow technologies. Specifically, they need a platform that provides collaboration and automation of risk and compliance processes.
3. **Enterprise applications.** Next, organizations look to further automate control monitoring and enforcement alongside the measurement of risk by gathering information directly from enterprise applications (e.g., financial systems for SOX compliance, credit or market systems within banking systems, manufacturing and logistic information within ERP systems, and training and qualification through HR systems).

4. **Business intelligence/business analytics.** Finally, after solving the content, process, and enterprise integration challenges of risk and compliance, firms must tackle reporting and communication requirements through business intelligence and business analytics features.

MAKING SENSE OF A FRAGMENTED GRC SOFTWARE PLATFORM MARKET

Large vendors have just started to enter the GRC software platform space to capitalize on their brands or sell more existing products, and small vendors see the market as virgin territory in which to make their marks. The result? More than 64 vendors can claim to provide at least some of the functionality required for policies/controls, assessment, analytics, and loss/investigations. Because these products' strengths and weaknesses still reflect their origins, we categorize them as:

1) purpose-built applications designed specifically for GRC; 2) enterprise content management (ECM); 3) business process management (BPM); and 4) enterprise applications (EA).⁷ These categories align closely with the previous four areas of technical functionality (EA, ECM, BPM, and BI/BA). However, Forrester doesn't include BI/BA software as a separate category here because vendors in the other areas typically form alliances with leading BI/BA software vendors to integrate BI/BA functions into their offerings.

Purpose-Built Software Provides Specific GRC Depth

Purpose-built applications pioneered the GRC market and continue to dominate it. In total, 49 vendors offer GRC software platform solutions (see Figure 7). This is because purpose-built applications:

- **Overcome the development and integration challenge.** As mentioned, a GRC platform spans four technical areas. Purpose-built applications ease the burden of building your own solutions on the components of other technologies like ECM and BPM. They provide an integrated solution, extending to broader enterprise systems where needed, that's specifically designed for GRC business processes.
- **Span risk and compliance areas.** The 49 vendors enter GRC from many different angles. Some vendors are specifically designed to be an enterprisewide GRC platform (e.g., Axentis, BWISE, IBM, Cura). The majority of these vendors are focused in particular areas of risk and compliance such as Sarbanes-Oxley (e.g., OpenPages, Certus, Paisley), quality in ISO 9000 (e.g., IBS Software), operational risk management (e.g., Ci-3, Strategic Thought), information security (e.g., Archer), or industry specific risk and control areas such as GMP in pharmaceuticals (e.g., MetricStream, QUMAS). All realized their applicability in the specific areas they focused on to be adaptable to an enterprise platform for GRC.
- **Are the most flexible.** While there is risk associated with buying software from a smaller firm in the purpose-built application GRC space, there is also opportunity. This area of the market is the most responsive to client demands, and vendors like Axentis, OpenPages, and QUMAS provide greater GRC depth than large software companies in the GRC software platform market.

Figure 7 GRC Software Platforms: Purpose-Built Applications

Vendor	GRC software	Policy/controls	Assessment	Analytics	Loss/investigations
80-20 Software	Leaders4	●	●	●	●
Achiever Business Solutions	Achiever Plus	●	●	●	●
Amadeus	Amadeus Compliance Process Control Suite	●	●	●	●
Archer Technologies	Archer Smartsuite Framework	●	●	●	●
Asparity Decision Solutions	J-Port Suite	●	●	●	●
Axentis	Axentis Enterprise	●	●	●	●
Business Propulsion Systems	BPS Server	●	●	●	●
BWise	BWise	●	●	●	●
Certus	Certus Governance	●	●	●	●
Ci-3	Sword	●	●	●	●
Compliance 360	Compliance 360	●	●	○	●
Cura Software Solutions	Cura Enterprise	●	●	●	●
Datacare Software Group	Global Corporate Manager	●	●	○	●
ember ec3	ember.HeatShield	●	●	●	●
EthicsPoint	EthicsPoint Online Training and Care Management	●	○	○	●
EtQ	EtQ Reliance	●	●	●	●
FRS	FRS FinancialAnalytics	●	●	●	●
Guideline	Risk Universe Business Intelligence	○	●	●	●
Hitec Laboratories	CONFORM	●	○	○	○
Horwath Software Services	Magique	●	●	●	●
IBS America	CompliantPro	●	●	●	●
i-flex	Reveleus Operational Risk	●	●	●	●
ISG Novasoft	Risk Management Compass	●	●	●	●
Keane	Keane SCORE	●	●	○	○

● Particular capabilities ● Basic capabilities and/or components ○ No capabilities

40037

Source: Forrester Research, Inc.

Figure 7 GRC Software Platforms: Purpose-Built Applications (Cont.)

Vendor	GRC software	Policy/controls	Assessment	Analytics	Loss/investigations
LRN	Legal Compliance and Ethics Center	●	◐	○	●
Mantas	Mantas Behavior Protection Platform	◐	○	○	◐
MediRegs	ComplyTrack	◐	●	◐	●
Methodware	Enterprise Risk Assessor	◐	●	●	◐
MetricStream	Enterprise Compliance Platform	●	●	○	●
Mitratach	TeamConnect GRC	●	◐	◐	●
OpenPages	OpenPages ORM	●	●	◐	●
Optial UK	Optial OpRisk Platform	●	●	◐	●
Paisley Consulting	The Paisley Solution	◐	●	◐	●
Pentana	Pentana	◐	◐	◐	◐
Prodiance	Prodiance Enterprise Compliance Platform	◐	◐	◐	◐
Protiviti	Protiviti Governance Portal	●	●	◐	●
QUMAS	QUMAS Compliance Suite	●	●	◐	●
Raft International	raft radar	◐	◐	◐	◐
Resolver	Resolver*Risk, Resolver*Net, Resolver*Ballot	●	●	◐	◐
Resources Global Professionals	PolicyIQ	●	◐	○	◐
Resultor	Resultor Enterprise Compliance	●	○	○	○
ROME Corporation	ROME OpRisk	○	●	◐	●
Ruleburst	Oasis	●	●	◐	●
Rulesphere	AEM Compliance Suite	●	●	◐	●
RVR Systems	RVR Regulatory Compliance	●	●	◐	○
Securac Holdings	Acertus Governance, Acertus RAC, MIMS	◐	●	◐	●
Strategic Thought	Active Risk Manager (ARM)	◐	●	●	●
Syfact	SYFACT Investigator	◐	◐	○	●
Symb	Aptius Risk Framework	◐	●	●	◐

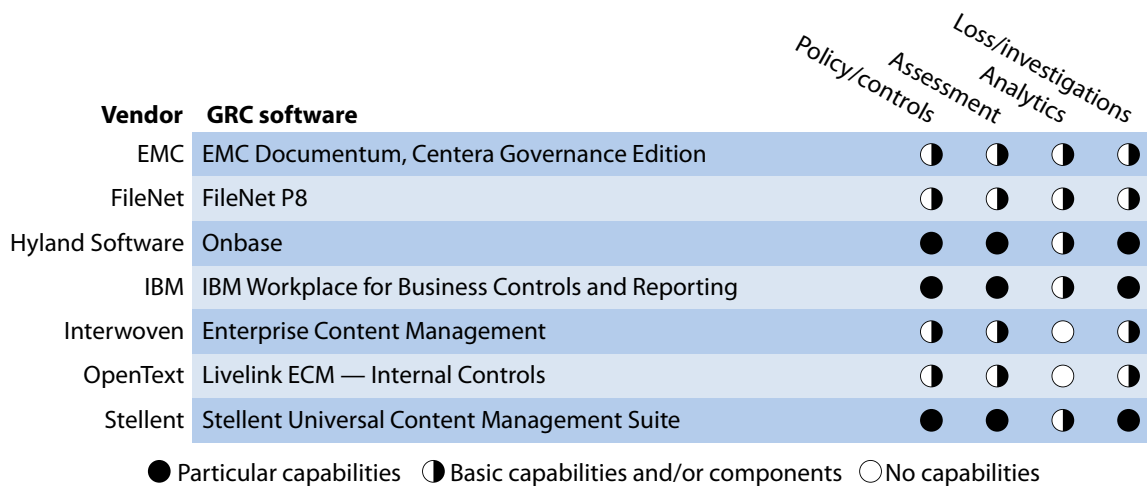
● Particular capabilities ◐ Basic capabilities and/or components ○ No capabilities

ECM Software Provides The GRC Backbone

Much of GRC software platforms’ functionality boils down to content and workflow. Risk assessments, compliance examinations, control assessments — in the end, all of these require firms to produce information. To manage risk and compliance well requires detailed content management and publishing capabilities combined with workflow. ECM players have been quick to learn this, and customers have built their own risk and compliance applications on top of ECM software for years.⁸

- **ECM vendors take one of two distinct approaches to the market.** While all ECM vendors attempt to address GRC, there are seven ECM vendors that specifically target messages toward the GRC software platform market (see Figure 8). EMC, OpenText, InterWoven, and FileNET concentrate on providing the content infrastructure for customers who want to build their own GRC applications. In contrast, Hyland Software and Stellent offer purpose-built applications on top of their own solution that they’ve acquired or built themselves.
- **ECM GRC opportunities will continue to grow.** Expect more acquisitions and partnerships — for example, EMC is already partnering with Paisley to bridge the gap between content and purpose-built applications — over the next several years. Forrester believes that ECM players like Stellent, OpenText, InterWoven, and FileNET will be acquiring purpose-built software to make their enterprise content repositories more attractive.

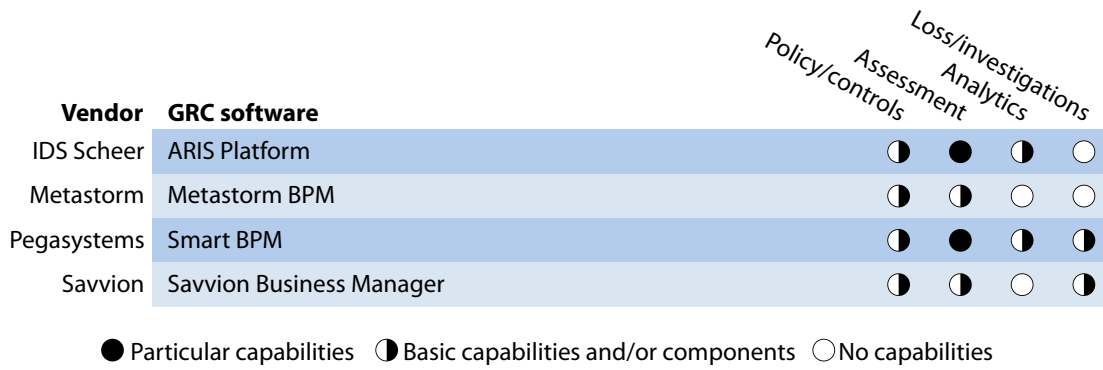
Figure 8 GRC Software Platforms: ECM Vendors



40037

Source: Forrester Research, Inc.

Figure 9 GRC Software Platforms: BPM Vendors



40037

Source: Forrester Research, Inc.

BPM Is A Sleeping GRC Giant

GRC software platform buyers have mostly emphasized content management and simple workflow, but four BPM vendors have ventured into the space (see Figure 9). Of these four, IDS Sheer has been the most aggressive:⁹

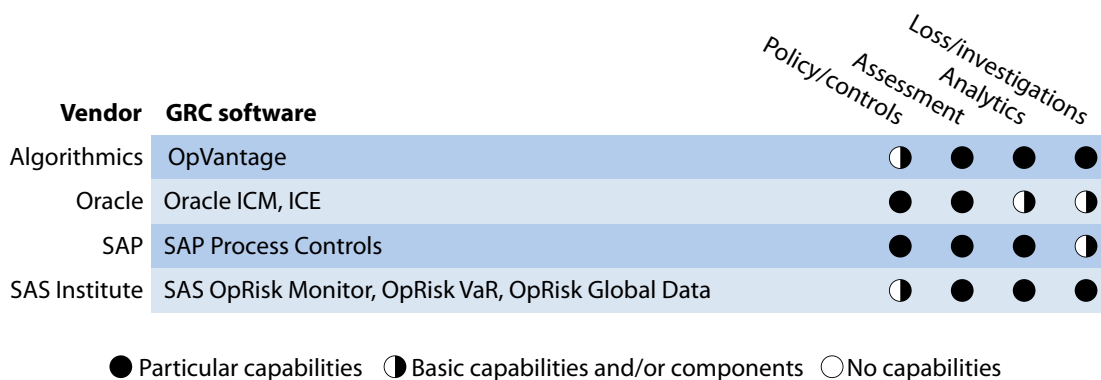
- **GRC platform buyers will realize the importance of BPM capabilities.** As firms define their GRC organizational structures and processes, BPM vendors can capitalize on the opportunity to integrate and manage GRC within business processes. IDS Sheer has been the most aggressive BPM player focusing on the GRC market.
- **BPM risk and compliance offerings will further expand to business rules engines.** As organizations invest in GRC software in the next few years, they will look for further capabilities to directly integrate, monitor, and enforce controls within business systems and processes.

Enterprise Applications Provide True Integration Of GRC

Enterprise applications provide the muscular and skeletal frameworks for business operations. Of the enterprise apps vendors, Algorithmics, Oracle, SAP, and SAS Institute are quickly closing in on the GRC software platform market (see Figure 10):

- **Enterprise applications vendors have had different approaches to GRC.** SAS and Algo have targeted specific verticals such as financial services with risk and compliance solutions for several years and are currently enhancing their solutions aimed at the GRC software platform space. Oracle and SAP have been slower to react, but SAP’s recent acquisition of Virsa indicates that it is aggressively pursuing the GRC software space with an intention of leading it.

Figure 10 GRC Software Platforms: Enterprise Applications



40037

Source: Forrester Research, Inc.

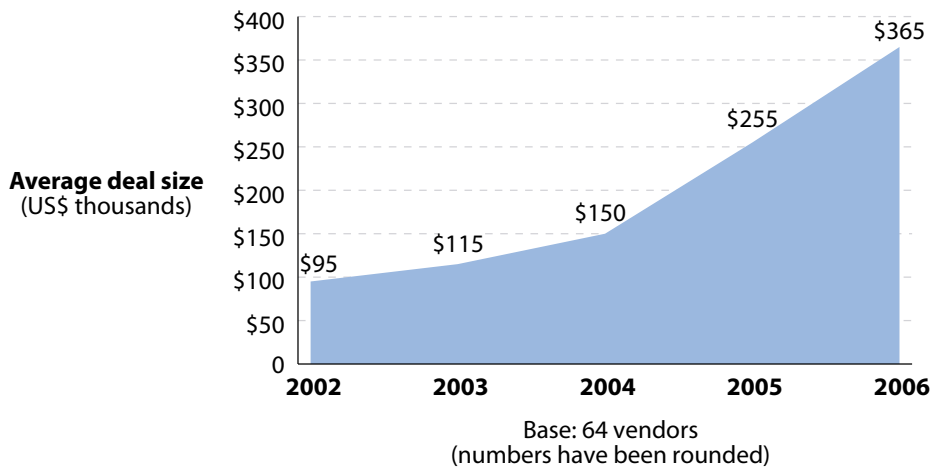
- **Enterprise applications’ integration of GRC provides future market opportunities.** Forrester expects the enterprise application vendors to take the lead in GRC in the next five years. While enterprise integration exists only for some purpose-built applications in this space, firms will need broader integration as they pursue further automation of risk and control monitoring and enforcement within their enterprise applications.

Some Firms Have Already Turned To Technology To Help Them Gain Control Of GRC

Leading organizations are already correcting risk and compliance myopia by centralizing oversight of risk and compliance under the CCO/CRO’s office and its technology investments:

- **International financial services firm adopts single GRC software platform.** In response to pressures of SOX and Basel II — with Solvency II just around the corner — this firm’s CRO listened to the business. The business was telling the CRO to implement technology to enable the GRC process, provide consistency in approach, and relieve the strain of repetitive assessments asking them the same questions.

Prescription: In response, this firm implemented the B Wise platform as part of its ERM program that was built to streamline consistency and efficiency into the risk and compliance processes. Its international lines of business were happy; the new platform reduced the amount of time they had to spend compiling risk and compliance information and gave them back information that proved valuable for risk reduction and control management.

Figure 11 GRC Software Platform: Average Deal Size

40037

Source: Forrester Research, Inc.

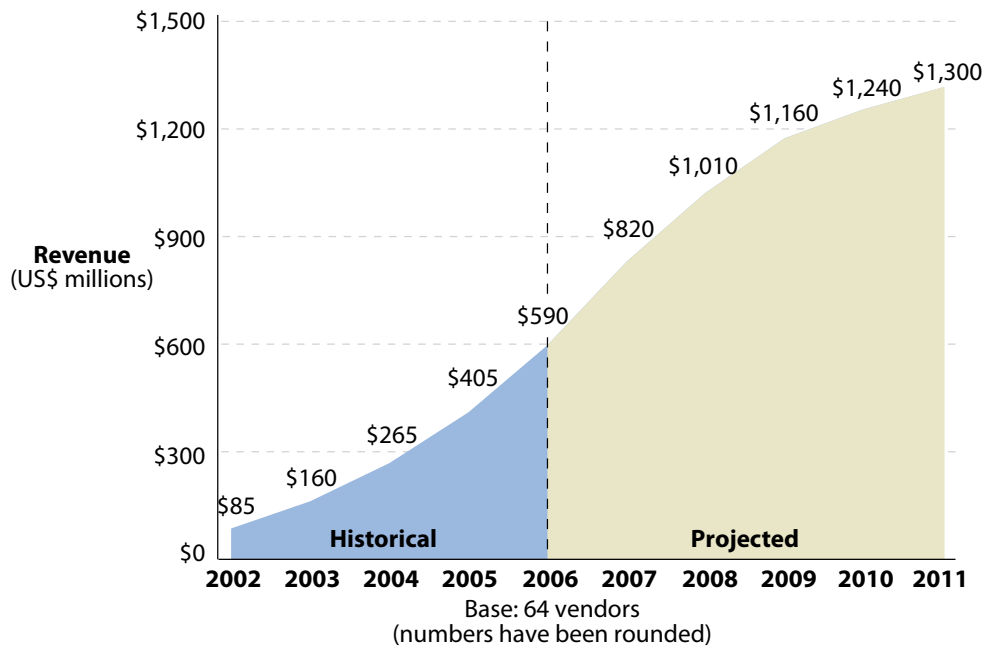
GRC SOFTWARE PLATFORMS: THE NEXT FIVE YEARS

The GRC software platform market came into its own in 2002. Before that, it was a variety of applications that focused on silos of risk and compliance. The average GRC software platform deal size has increased from \$95,000 to \$365,000 in software revenues (see Figure 11). Customers typically pay an additional 30% to 50% of the software cost for implementation services. The growth in deal size coincides with a shift from the use of these platforms for a tactical regulatory/risk purpose such as SOX compliance to enterprise GRC. The expanded user base for enterprise GRC has driven some deals in this space to as much as \$4 million in large environments.

GRC Software Platform Revenues Will Rise To \$1.3 Billion In 2011

Coinciding with the growth in deal size, since 2002, the revenues of the 64 vendors that Forrester includes in the GRC software platform market have grown from a total of just \$85 million to \$405 million in 2005 (see Figure 12).¹⁰ The primary drivers for this growth have been Sarbanes-Oxley, Basel II, and other regulations, as well as firms' focus on developing enterprise risk management programs to deal with diversified and distributed business risks.

The GRC software platform market will continue to grow steadily over the next four years in further response to risk and compliance pressures around the world. Forrester expects the market for GRC software platforms to climb to \$590 million in 2006, and we predict that it will reach \$1.3 billion in 2011. If enterprise risk and compliance management becomes a defined business process within most firms, this estimate will prove conservative:¹¹

Figure 12 Forecast: US GRC Software Platforms: Software Revenue Market Size, 2006-2011

40037

Source: Forrester Research, Inc.

- **2007 and 2008 are the high growth years.** As companies put in place their long-term GRC solutions, Basel II kicks in, and risk management really starts to take hold in large enterprises. The GRC market will grow explosively in 2007-2008 and will start to plateau around 2010.
- **Future growth will hinge on firms migrating to integrated views of risk and compliance.** The early years of this market focused on a single point of pain such as environmental health and safety, but the aggressive growth of 2007-2008 will come from enterprise risk and compliance. Average deal sizes will continue to grow as organizations expand their implementations to cover broader risk and compliance domains.
- **The broader risk and compliance market is huge.** This forecast focuses on the GRC software platform market that we defined in this document. However, there are many other areas of risk and compliance. Overall risk and compliance spend on software is several factors greater than what is measured for GRC software platforms alone.

GRC Software Platform Growth Drivers Through 2011

GRC software technology will continue to evolve and expand as the market matures. Here's how:

- **Risk and regulatory intelligence.** GRC systems have the content and processes to manage current compliance requirements and today's defined risk metrics. However, customers will

need systems to integrate more intelligence capabilities to monitor new developments. In the compliance world, this means profiling the regulatory/legal environment and tapping into legal intelligence services such as Lexis or WestLaw to identify new court rulings, laws, and regulatory changes. Shifts in risk and new regulations will kick off a process to review the impact on the organization and propose potential changes of controls; Compliance 360 gives customers some of this functionality today. In the risk world, firms will need GRC software platforms that help them identify economic, environmental, or political events that may affect business processes.

- **Risk analytics and visualization.** The majority of the vendors in the GRC market have not focused on the mathematical models and engines that can do complex risk simulation. Thus, they'll need to acquire specialist vendors like Strategic Thought and Methodware; financial services customers will be first to demand sophisticated risk analytics, but others will follow. Risk visualization and dashboarding technologies are also hot areas that will differentiate vendors over the next few years.
- **Business rules engines.** Successful GRC requires integration into business processes. For the next five years, customers will want risk and compliance features incorporated into business logic/rules engines to enforce controls and route process events given specific risk and compliance scenarios. Both BPM and business rule engine vendors will profit as the market moves in this direction starting in 2007.
- **Enterprise integration.** Finally, the GRC software platform needs to extend to enterprise systems and applications. Enterprise vendors like SAP and Oracle are seeing this trend and are defining their GRC strategies. Because enterprise applications drive business processes, GRC software must integrate with these systems so that it can collect information and automate GRC controls and processes.

RECOMMENDATIONS

DEFINE YOUR RISK AND COMPLIANCE ARCHITECTURE

A GRC software platform is not a silver bullet to risk and compliance — no technology is. But don't despair; here are the steps to start with:

- **Start with defining your GRC vision.** For organizations to successfully use these platforms, they need to start with defining the scope and vision for GRC within their enterprise. Organizations must decide if compliance and risk management will remain separate domains or be integrated under a single executive. Interestingly, operational risk management and compliance have nearly identical taxonomies and processes.

- **Develop your long-term strategy for GRC.** Once you have a vision, you can build a strategy to execute on that vision. Focus on organizational structure, people, and processes first, and *then* start thinking about implementing a GRC software platform.
- **Be selective in the platform you choose.** The market is crowded with many vendors hawking their wares. To make the best investment in a space that is bound for growth and consolidation of players, customers need to understand the stability, customer satisfaction, and partnerships as well as industry-specific experience of the GRC vendors they are evaluating.
- **First get your feet wet.** Organizations need a road map for implementing a broad GRC vision. Don't take on too much by trying to swallow the ocean. Start with one or two risk and compliance areas and expand the solution to encompass others over time. For many facing the current pressures of SOX, this will mean implementing a GRC software platform for this purpose today and expanding it to others tomorrow.

ALTERNATIVE VIEW

GROWTH CONTINUES TO SKYROCKET IF GRC EXPANDS TO BUSINESS PERFORMANCE

Risk management, if done right, relates closely with business performance. Further, compliance is really about selecting the right level of controls, not just to meet requirements, but also to manage business operations. As GRC takes hold in organizations, there is a potential trend for greater GRC software platform growth if it delivers on the business performance message. The net effect of this would be to increase the growth rate for GRC software platforms and keep the curve from flattening in 2010-2011.

SUPPLEMENTAL MATERIAL

Companies Interviewed For This Document

80-20 Software	i-flex
Achiever Business Solutions	IDS Scheer
Algorithmics	Interwoven
Amadeus	ISG Novasoft
Archer Technologies	Keane
Asparity Decision Solutions	LRN
Axentis	Mantas
Business Propulsion Systems	MediRegs
BWise	Metastorm
Certus	Methodware
Ci-3	MetricStream
Compliance 360	Mitratach
Cura Software Solutions	OpenPages
Datacare Software Group	OpenText
ember ec3	Oracle
EMC	Optial UK
EthicsPoint	Paisley Consulting
EtQ	Pegasystems
FileNet	Pentana
FRS	Prodiance
Guideline	Protiviti
Hitec Laboratories	QUMAS
Horwath Software Services	Raft International
Hyland Software	Resolver
IBM	Resources Global Professionals
IBS America	Resultor

ROME Corporation	Savvion
Ruleburst	Securac Holdings
Rulesphere	Stellent
RVR Systems	Strategic Thought
SAP	Syfact
SAS Institute	Symb

ENDNOTES

- ¹ Pharma companies are regulated throughout the business cycle from product development and approval, manufacturing and distribution, to marketing and promotion of pharma products. Forrester analyzed the risk and compliance burden on pharma companies. See the April 24, 2006, Best Practices “[Pharma Risk Managers: ERM Is In Your Future.](#)”
- ² Consider the impact on businesses around the world responding to environmental threats of the tsunami, hurricanes, and earthquakes alongside preparing for potential flu pandemics.
- ³ The US Office of Information and Regulatory Affairs, part of the Office of Management and Budget (OMB), 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 The Cato analysis is found in an annual report it publishes on the impact of federal regulations called “Ten Thousand Commandments: An Annual Snapshot of the Federal Regulatory State.” Specifically, the report details, “Based on a more broadly constructed competing compilation of annual regulatory costs by economists Thomas Hopkins and Mark Crain, regulatory costs hit an estimated \$869 billion in 2002, an amount equivalent to 40 percent of all FY 2003 outlays.” Source: Clyde Wayne Crews Jr., “Ten Thousand Commandments: An Annual Snapshot of the Federal Regulatory State,” Cato Institute (http://www.cato.org/tech/pubs/10kc_2004.pdf).
- ⁵ The Open Compliance & Ethics Group (www.oceg.org) is instrumental in developing a framework illustrating the breadth of GRC issues that organizations face. The OCEG effort is taking a cross-industry look at GRC to develop an expansive and cohesive framework that includes:

International transactions: foreign negotiation and sales, antiboycott/export controls, economic embargoes, global trade and competition.

Corporate governance: board structure and processes, audit committee structure and processes.

Intellectual property: copyright, trademark, trade secret, patent.

Competitive practices: antitrust, customer/competitor/supplier relations.

E-compliance: electronic info, email and postings, Internet security, Internet privacy.

Ethics: conflicts of interest, ethical decision-making, gifts and gratuities, respectful conduct.

Information management: document retention/records management, electronic data management, information security, information privacy.

Emergency preparedness: business continuity, disaster recovery.

Employment: anti-discrimination/accommodation, anti-harassment, benefits, compensation, contingent workforce, employee privacy, executive compensation, global mobility/immigration, hiring/retention, labor, leaves of absence, retaliation/whistleblowing, substance abuse, terminations and RIFs, torts, workplace violence.

Government dealings: government contracts, political activity/government relations.

Environmental: environmental management, hazardous material handling, environmental reporting, permit management.

Workplace health/safety.

Product quality/liability.

Fraud and corruption: insider transactions, money laundering, foreign negotiation and sales, revenue and expense recognition.

⁶ The spectrum of compliance challenges that organizations are up against encompasses governance, employment, financial assurance, antifraud, information management, intellectual property, environmental, international dealings, competitive practices, product quality/safety, workplace health/safety, and government dealings.

⁷ Figures 7 through 10 illustrate the vendors' broad capabilities in the four GRC capability areas. These graphics are not to be interpreted specifically as competitive differentiators as each vendor has specific strengths and weaknesses in GRC features as well as industry focus. For a more thorough comparison and competitive differentiation of 10 of the 64 vendors in the GRC software platform market, there is a Forrester Wave evaluation of GRC platforms. See the March 16, 2006, Tech Choices "[The Forrester Wave™: Governance, Risk, And Compliance Platforms, Q1 2006](#)."

⁸ Forrester evaluated ECM vendors and their preparedness to support content-centric applications like compliance in the Forrester Wave evaluation of content-centric applications. See the March 29, 2006, Tech Choices "[The Forrester Wave™: Content-Centric Applications, Q1 2006](#)."

- ⁹ Forrester identifies that numerous compliance challenges are key drivers for BPM market growth in 2006. Forrester recognizes compliance as a driver of business rules engines and evaluates the Leaders in this space in a Forrester Wave evaluation of business rules engines. See the January 26, 2006, Market Overview [“Demand For Business Process Management Suites Will Accelerate Through 2009”](#) and see the January 4, 2006, Tech Choices [“The Forrester Wave™: Business Rules Platforms, Q1 2006.”](#)
- ¹⁰ To model the market, Forrester worked with the software revenues of the 64 vendors reported under NDA. Where necessary, when too little or no information was shared, Forrester estimated revenues.
- ¹¹ Note: These estimates are specifically for the software revenue of the GRC software platform market and do not represent further spend on single compliance initiatives or overall spend on enterprise risk and compliance software.

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.