Aite PARTNER. ADVISOR. CATALYST.

Governance, Risk, and Compliance: Smooth Seas Do Not Make Skillful Sailors

Prepared for:

MetricStream

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

If information is power, now is the time for risk and compliance technology tools to proactively defend companies. Across the corporate hierarchy, the regulator's spotlight is on key constituents' information awareness. Game-changing regulation and client scrutiny mean a new business landscape for companies, and it is clear that centralized information feeds intelligent decision-making. Financial services firms are in high gear to meet regulatory obligations and earn back trust. It's a bumpy ride but in the end will be beneficial to more than just the financial services sector. As an old proverb states, "smooth seas do not make skillful sailors." Everyone hopes that when this storm subsides, the key learning in corporate oversight will hold the industry back from another financial-crisis-like precipice.

To accomplish the task, senior management must develop a risk-conscious culture within the firm. Companies must define their risk appetite and communicate to employees the necessity and purpose of staff in governance, risk, and compliance. Too many shocking news headlines have stunned the industry and its clients. The new corporate oversight initiatives call for all hands on deck.

Governance, risk, and compliance (GRC) is an umbrella term referring to an organization's overall approach to policies and procedures and internal controls. These requirements span the interrelated areas of governance, risk, and compliance. "Governance is the act of externally directing, controlling, and evaluating an entity, process, or resource. GRC is a capability that enables an organization to reliably achieve objectives while addressing uncertainty and acting with integrity."[1]

Generally speaking, risk and compliance software is a highly fragmented market, and point solutions often address a single regulatory challenge when many dozen exist. Vendors and service providers often seek to help clients manage the workload with incremental additions to their solution functionality or service. For example, a solution or service assisting with Form PF is expanded to support the Alternative Investment Fund Managers Directive or other specific regulation. Yet the expansion tends to be a painstakingly slow process that lacks scalable applications to other new regulation. Often, because these solutions were not intended as comprehensive risk and compliance platforms, they do not meet the risk and compliance team's priorities and workflow. This type of patchwork support for the function has risk and compliance teams dependent on other divisions for the information their jobs require. GRC software aims to bring GRC teams' many responsibilities into one tightly run ship.

This white paper looks at the environment for GRC technology within the financial services industry. It discusses the challenges and benefits of the technology and the latest developments affecting adoption.

1. "Governance," Open Compliance and Ethics Group, accessed May 7, 2014, www.oceg.org/category/theme/governance.

METHODOLOGY

In early 2014, Aite Group interviewed strategy staff, product managers, implementation representatives, and sales managers among 10 vendors serving the financial services industry. Interview topics focused on key business trends and challenges, client requirements, and the evolution of their systems. Six vendors participated in a solution survey for Aite Group's GRC note. Aite Group also held product demos and follow-up interviews and conducted interviews with buy-side firms to capture direct user analysis and industry feedback and insights.

MARKETPLACE

Aite Group's 2011 analysis on GRC platform adoption concluded that vendors in this market face several challenges:[2]

- Educating clients on what a comprehensive GRC can do
- Establishing greater resolve with the client for change management, shifting employee mindsets to move off manual, Microsoft Excel, and email processes
- Quickly helping clients who do not have a GRC framework in place
- Speeding implementations so clients can absorb the solution benefits within a short time frame
- Avoiding complex implementations that get bogged down by a lack of client focus, framework, or internal agreement
- Keeping the platform competitive via a user-friendly interface, modern technology, and open systems

Financial firms need to treat GRC platforms as a strategic corporate initiative. The effort requires a top-down commitment from the executive office to champion the solution.

Integrating GRC into the fabric of a company can happen gradually—many implementations begin in one area of the firm, such as audit or IT risk, and then extend to other departments. But different business functions' perspectives on the business can clash, and a disagreement can manifest as multiple GRC platforms at one firm. A common example of different perspectives is the audit team's focus on controls and the operational risk team's focus on specific risks.

Though these teams may wish to devise their own taxonomies, prioritize differently, and employ separate workflows, for consistency and clarity, a firm should use an overarching taxonomy that everyone agrees on. If this is politically a nonstarter for a firm, a solution may support the use of different field names for the same item and allow users to view the fields by a functional user profile. Ultimately, all the data would align to a firm-wide nomenclature and viewpoint.

2. See Aite Group's report *Governance, Risk, and Compliance Platforms 2011: Accountability and Integrated Oversight*, January 2011.

WHY ADOPT A GRC PLATFORM?

Who uses GRC platforms? The largest firms in any financial services subsector, including investment banks, banks, insurance companies, asset managers, and large alternative funds use GRC platforms. Examples of firms using GRC include AIB, Barclays, BlackRock, Citi, Credit Suisse, GE Capital, Pimco, State Street, T. Rowe Price, UBS, and Vanguard. Vendors hold client lists highly confidential, yet it's widely accepted that at least the top 50 in any of these sectors are using a platform in some capacity.

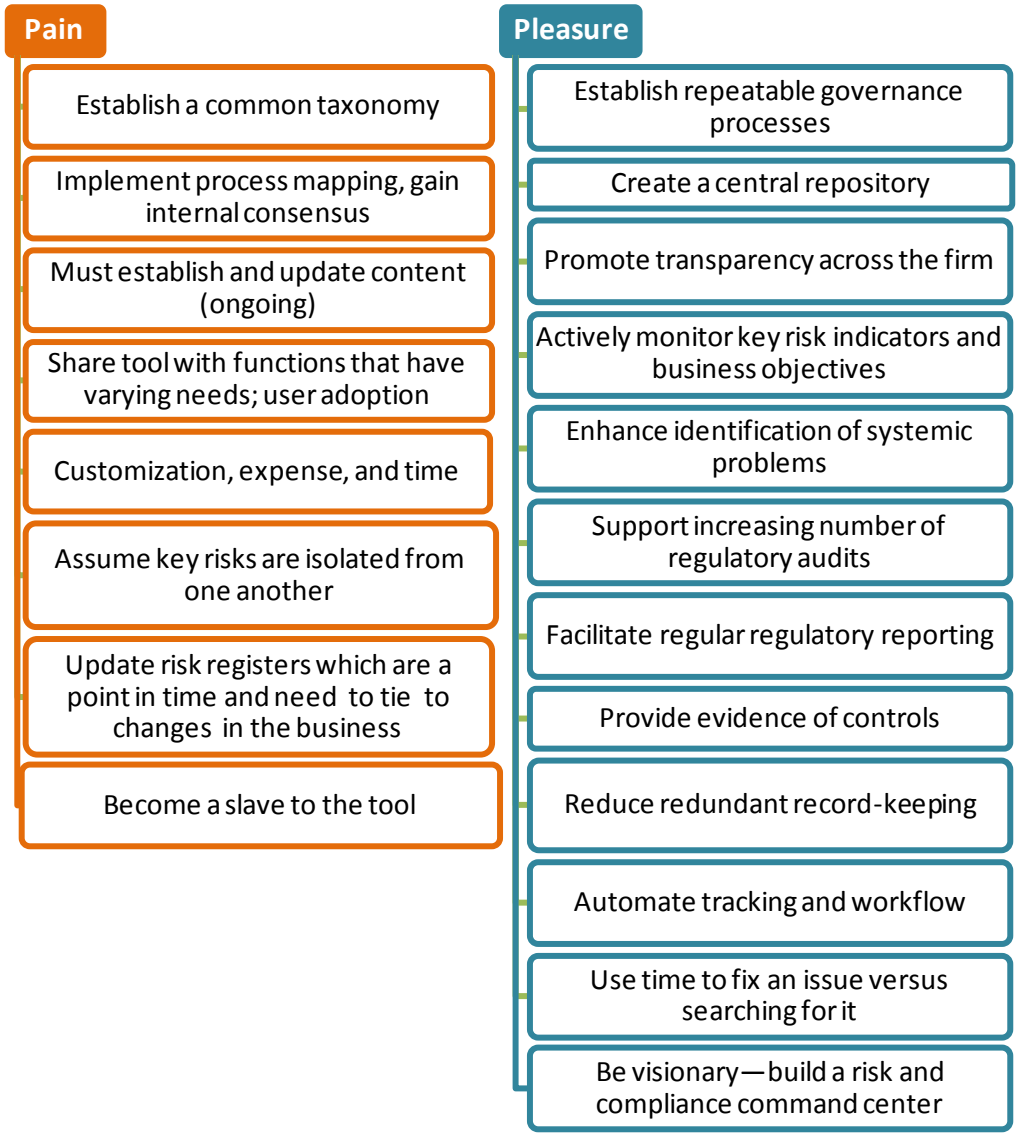
The business environment is complex. Global firms manage disparate jurisdictions and regulations, business lines, products, types of client markets, and dispersed staff in multiple offices, all of which require supervision and integrated oversight. Corporate governance seeks to provide a fair return to investing shareholders and to operate legally and ethically. This involves a system of checks and balances, including a board of directors, an external auditor, and internal systems and controls for accountability and management (e.g., compensation, supervisory hierarchies, policies, and procedures).

While one could argue that GRC adoption is more inspired by the regulatory environment than by the general business environment, today's business demands require a clear, integrated approach to corporate oversight. Coupled with heightened business and market momentum, an abundance of information requires probing analysis. The business climate calls for earlier warnings of issues the firm must handle. The firm's profitability, and quite possibly its longevity, is at stake. On all fronts—from investor to employee to client to regulator—firms' constituent bases have increased their expectations about financial services firms' automated controls and efficiency.

Figure 1 provides a glimpse into the pain and pleasure that firms have experienced while deploying GRC platforms. Historically, financial firms purchasing the more prominent platforms have frequently relied on consultants to create a unique experience with the platform by customizing workflows and screens. In the end, this has led to expensive implementations and ongoing platform updates.

The environment continues to change. As vendors streamline implementations and grow in their knowledge of financial services workflows and business requirements, they build solutions better suited to that market. It's no easy task, as the players vary, and the environment of an institutional asset manager is quite different from that of a universal bank.

Figure 1: Two Sides of the Coin—the Pain, the Pleasure



Source: Aite Group

KEY CHALLENGES FOR GRC CLIENTS

The GRC platform is a single repository of critical information that allows a company to map a framework to document, monitor, manage, test, and report on the firm policies, processes, key business risks, issues, controls, and corrective action plans across a hierarchy of business entities. The information repository is dynamic; changes are based upon regulation or firm policy change, changes in products or markets, operational processes, crisis events, or other situations that arise.

What prompts use of a GRC platform? Most frequently, a particular business need drives firms to adopt the platform. For example, a financial services firm might initially seek a solution to cope

with the rising number of third-party vendors that require due diligence and tracking. Alternatively, a firm may have the solution in place for a particular area, such as IT risk or Sarbanes-Oxley compliance, and seek the same vendor's support to roll out an additional module for the new business need such as business continuity. Firms may also take action in response to a regulator's action against them or a failed audit, fine, or penalty. GRC staff at client companies are closely watching competitors that are in this uncomfortable situation and are taking steps to avoid a similar scenario.

Vendors were asked to describe key challenges observed for clients adopting a GRC solution. The most frequently cited challenges include the following:

- Lack of customer readiness or organizational structure to support GRC processes
- Lack of client executive sponsorship
- Lack of common terminology to establish a GRC framework: for example, risk's "risk-mitigation strategies" and audit's "internal controls"
- Overindulging in process automation—getting carried away with the tool
- Implementing too many use cases at once
- Lack of buy-in from employees, stalling adoption
- Aggregation of data from multiple sources
- Failure to identify and commit to a power user to administer GRC

Vendors recommend clients begin with the end in mind, understanding what management reporting will lead to actionable information. Well-defined management reports demonstrate the value of a GRC solution through relevant and timely risk intelligence.

Users should understand how the tool should be used—to align different GRC processes from across the organization to a common framework of risk registers, objectives, controls, and policies and therefore better govern the business.

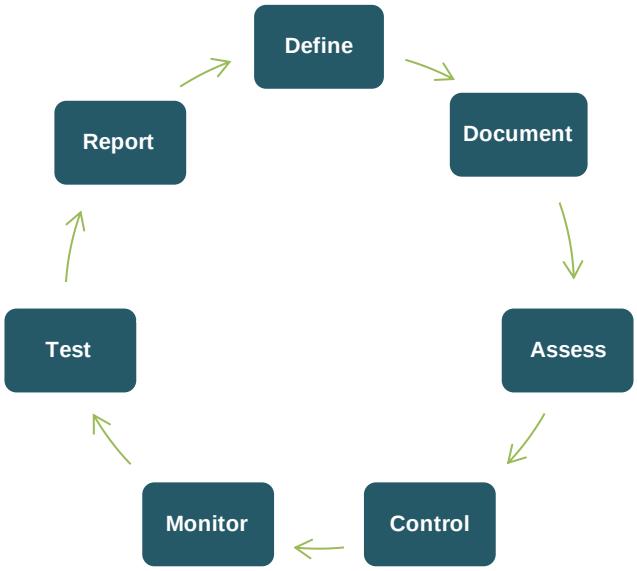
As such, it requires collaboration among employees. Recognize that GRC is a change management event at the firm. The initiative touches many employees as users or beneficiaries and requires staff buy-in for success. The implementation is as much about people and communication as it is risk and control frameworks. Ultimately, a GRC as a resource of information, owned by all, makes for eager participants.

Both vendors and clients observe that the biggest implementation challenges for prospective GRC clients are internal to the company. Employees must act collaboratively to successfully use a GRC to its fullest extent. Multiple stakeholders must agree to common taxonomies and business processes as well as key risks, controls, and process owners. Further, each firm must clearly define its business terms, data policies, data standards, data quality rules, data quality metrics, and master data rules.

In the GRC environment (Figure 2), a firm will follow an iterative path over time to properly manage GRC programs. The solution supports the process with the tools the company needs,

including assessment surveys, calendars, document management, quantitative aggregations of errors or losses, what-if analysis, control and testing procedures, reporting, and (for some solutions) the ability to report on the trend experience of the organization. Workflow tools include scheduling, sign-offs, activity owners, and automated alerts. Firms typically derive dashboard views by functional role.

Figure 2: The Iterative Process of GRC Management



Source: Aite Group

AN INDUSTRY UNDER DURESS

The financial services industry faces an ongoing reputational crisis and massive doubt about its ability to act with integrity. In March of 2014, Forbes published its "America's 100 Most Trustworthy Companies 2014."[3] These firms demonstrate excellent accounting transparency, supervision by their boards of directors, and the lowest incidence of high-risk events. Notably, not one financial services firm is on the list.

Several financial services firms have demonstrated poor governance and wound up in news headlines. In 2014, Barclays, UBS, and Royal Bank of Scotland were fined a total of about US$6 billion for manipulating the London interbank offered rate, or Libor, and related benchmarks that underpinned about US$300 trillion worth of transactions worldwide. UBS' former trader was convicted of fraud after making unauthorized trades and listing fictitious transactions. The bank's internal controls failed to detect the trader's activities, and its global head of operational risk blamed the company's lack of timely information flows from the risk management subsystem to the supervisory portal. These firms are hardly alone. Other examples include the lending practices that generated the subprime mortgage crisis; the Bernie Madoff scandal, which

3. Forbes in conjunction with GMI Ratings. List was culled from 8,000 companies on U.S. exchanges with market capitalizations of more than US$250 billion. GMI Ratings evaluates 60 different governance and forensic accounting measures to create the list.

operated the largest accounting fraud in U.S. history; and the trader known as the London Whale, who lost more than US$6.2 billion for J.P. Morgan.

Corporate governance and enterprise risk management are not new corporate initiatives, yet these initiatives are often isolated within a company's IT, risk, and governance groups. Two common standards in the industry include the Committee of Sponsoring Organizations (COSO) ERM 2004 and the International Organization for Standardization (ISO) 31000:2009. In 2013, COSO published an updated framework.[4]

Most large and complex firms have policies and processes intended to provide corporate oversight and manage risk. Unfortunately, the 2008 financial crisis and the continued negative headlines regarding employee activities at large financial services firms makes it clear these are not good enough. Broadly speaking, governance issues often arise from the following:

- Human error, fraud, negligence, or failure to adhere to documented risk controls
- Compensation structures aligned with corporate objectives but not risk controls or risk appetite
- Lack of timely, centralized information
- Lack of automated systems and workflows

VENDOR RISK MANAGEMENT

Vendor risk management (VRM), also referred to as supplier risk management or third-party outsourcing, entails the process of building and executing a risk-control framework to validate the policies and controls at new and existing vendors that a firm uses to accomplish the firm's business goals. The aim is to understand how the vendor operates its business and internal controls so as to safeguard the firm and its clients from the vendor's potential failure to deliver the service or product or the vendor's exposure of highly confidential information (such as personally identifiable information). VRM searches for a potential threat to mitigate the firm's risk.

The regulatory spotlight is on VRM. Regulators, such as the U.S. Office of the Comptroller of the Currency and the banking industry's Federal Financial Institutions Examination Council, issue guidance on vendor assessments, typically in the form of topical lists. The specific detail of what is acceptable or not is left to the financial institutions to ascertain. Most financial institutions approach regulatory audits with some trepidation as to the regulators' interpretation of their program. The best defense is a VRM program that is doing the following:

- Communicating clearly its mission and concerns to employees
- Addressing risks consistently and effectively
- Repeatable and inclusive of all vendors

4. Guidance on Internal Control—Integrated Framework (2013), accessed May 7, 2014, http://www.coso.org/ic.htm.

- Documented end to end

Technology specifically for vendor risk management is relatively new to the market. A number of GRC solutions are only just adding a vendor risk management module. VRM often taps multiple resources to address program requirements; for example, they handle questionnaire administration through a procurement package, yet monitor and manage risks through a proprietary system or Microsoft Excel. Often, VRM piggybacks off platforms designed for other teams, which often means a lack of workflow accommodation for VRM staff. This is not likely sustainable given the volume of vendor deals, ongoing risk assessments, and regulation-required oversight of both the VRM program and the vendors.

VRM is a document-intensive job, not just in what is received from vendors, but what must be generated internally. Electronic copies are generally the best approach, and this is becoming easier in today's office environment, particularly with SharePoint. From a systems use perspective, a sampling of VRM daily activities could include viewing, examining, validating, creating, updating, or distributing the following:

- Vendor deal records
- Vendor profiles
- Supporting documentation from request for proposal to due diligence to contracts
- Vendor inherent risk classification
- Vendor risk-assessment results
- Vendor questionnaires
- VRM metrics reports
- VRM vendor list matched with accounts payable system
- Vendor manager interactions and support entries
- Ongoing vendor oversight documentation
- Vendor file notes/comments

VRM is fending off the onslaught of heavy risk assessments volume and the ongoing oversight. Technology solutions that can handle VRM workflow flexibly and manage the wide scope of VRM responsibility will be in demand. VRM budgets are thin but have the potential to adjust if a viable technology solution is available.

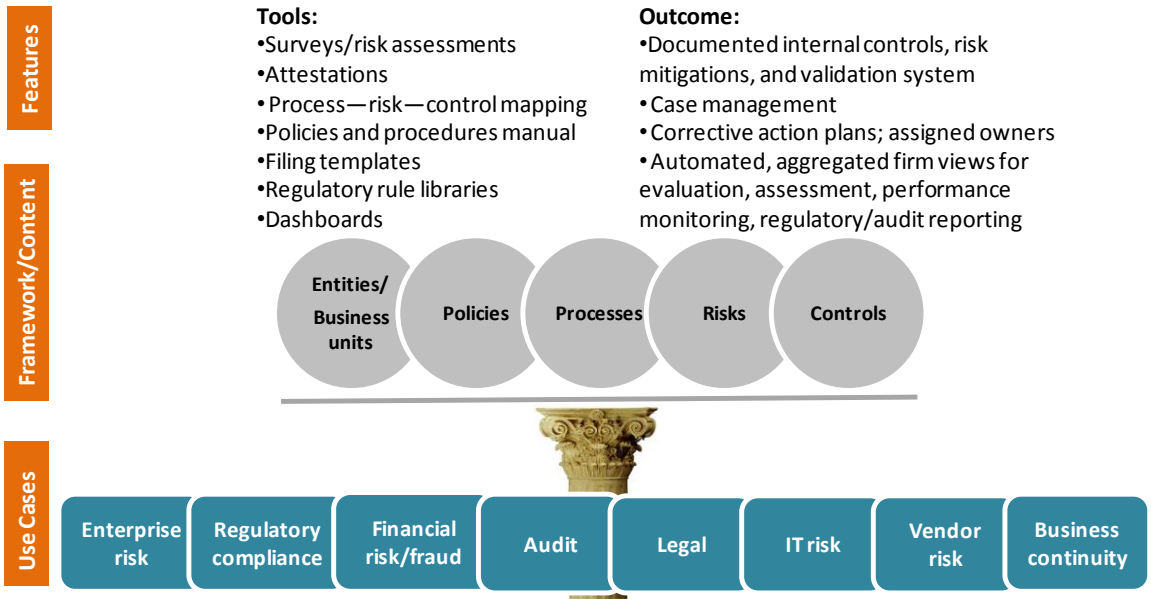
USE CASES FOR GRC SYSTEMS

There are several uses cases for GRC systems. The most all-encompassing is as an enterprise risk management (ERM) platform, which captures all aspects of GRC activities. The use cases are often presented as modules or components to the overall GRC platform, and the functionality

tools are typically available within each of the components. Figure 3 provides an overview of the various aspects of GRC platforms.

The GRC platform uses a process-based approach to link every functional area to the same GRC framework and the same definition of terms (or provide an ability to translate those terms to specific group preferences, when necessary). It is a centralized documentation and framework of business process, controls, and risk metrics. GRC frameworks are also referred to as the "risk register."

Figure 3: The GRC Platform—Use Cases, Content, and Features



Source: Aite Group

GRC CONTENT AND CONNECTIVITY

Establishing initial content is one of the biggest challenges for new users of GRC. If a firm has a well-documented ecosystem, it must upload numerous existing processes, policies, compliance controls, and so forth. For some firms, however, it means creating content. GRC vendors can help. They may provide proprietary or industry-standard content in the form of GRC frameworks and supply feeds for regulatory content, or they might have an established partner to provide such content. Clients can also utilize numerous third-party vendors, such as Open Compliance and Ethics Group (a nonprofit think tank) or Risk Business (a risk advisory firm), KPMG, Deloitte, or other consulting firms.

GRC platforms connect to a growing list of third-party resources for news, standards content, IT infrastructure performance, financial data, employee data, and other client-specific content. A sampling of resources include the following:

- **Real-time legislative and regulatory alerts** from various sources, such as the U.S. Securities and Exchange Commission (SEC), U.K. Financial Conduct Authority (FCA), the U.S. Financial Industry Regulatory Authority (FINRA), the international Financial

Stability Board, and third-party providers such as LexisNexis/Dow Jones, StateScape, European Research Council, and Thomson Reuters

- **Information security:** Qualys, Nessus, Rapid7, Symantec, AppDetective, Verdasys
- **IT system performance monitoring:** ServiceNow
- **Procurement systems**: Ariba (SAP), Bravo, Iasta
- **Human resources systems:** SAP, PeopleSoft
- **Financial analysis ratings:** Rapid Ratings
- **Content** from the client firm's data warehouse(s) or the firm's Microsoft SharePoint directory

Vendors that promote GRC's integration with other solutions and services will deliver a solution with greater ease of use, improved timeliness of information and, essentially, a connected world that prompts staff action.

Vendor solutions support connectivity methods including file uploads, XML feeds, and Web services application programming interfaces (APIs).

USE CASE: REGULATORY COMPLIANCE

The range of regulatory compliance is vast, particularly for firms operating in multiple jurisdictions. Keeping abreast of changes and updates is a difficult task for compliance officers who must also incorporate changes to relevant policies and procedures documentation. The regulation and industry best practice standards list below is a mere glimpse of the demands on financial services firms.

- **Financial reporting:** Sarbanes-Oxley in the United States, JSOX in Japan, Bill 198 in Canada
- **Governance:** COSO, ISO
- **IT risk:** ISACA 's Control Objectives for Information and Related Technology (COBIT 5), the United States' National Institute of Standards and Technology (NIST)
- **Corruption:** The U.S. Foreign Corrupt Practices Act (FCPA), the U.K.'s Bribery Act 2010
- **Human resources:** Occupational Safety & Health Administration (OSHA)
- **Internal controls:** The U.K. Financial Reporting Council's Guidance for Directors on the Combined Code (Turnbull Report)
- **Personal data:** the United States' Gramm-Leach-Bliley Act, the EU's Data Privacy Directive, and industry standards such as the Payment Card Industry Data Security Standard (PCI DSS)
- **Anti-money laundering:** The U.S. Bank Secrecy Act of 1970 and Patriot Act of 2001

- **Regulatory filings:** FINRA, the SEC, the FCA, the U.K. Prudential Regulation Authority

Compliance staff and senior management are best served with a centralized view of firm activity relative to regulatory compliance. Information and a plethora of spreadsheets moved off local hard drives to a centralized repository provides a workflow engine incorporating authorization processes, employee actions, alert notices, and so forth. This shifts the focus from log and track to regulatory intelligence and creates the ability to assess the impact of regulatory or firm changes, assign ownership, schedule, and take action.

Another way in which GRC solutions support regulatory compliance is with workflow engines supporting policy and procedure creation, maintenance, document version control, dissemination, and attestation—key required activities for core program management.

Compliance officers frequently interact with employees for training, attestations of company policies, and compliance assessments on the performance of internal controls. A GRC platform has notification tracking and questionnaire capabilities to communicate to relevant staff and record their responses. Users may even initiate situational compliance assessments, which enable differentiation based on specific scenarios. All the information is permanently stored.

Finally, GRC platforms support case or incident management—the tracking of regulatory issues with workflow escalations baked in and corrective actions assigned to staff. Reporting provides for metrics tracking and trend analysis as well as retention of historical details and relevant reporting for audits or inquiries.

USE CASE: ENTERPRISE RISK MANAGEMENT

Some say that ERM systems and processes are devoted to building firms' resilience. An ERM solution brings together all components and tools shown in Figure 3, from financial controls to operational risk to audits. Not all risks can be foreseen, but active and ongoing risk assessment helps an organization respond faster and rebound more effectively. The visibility of the GRC process and content in day-to-day work life educates employees on developing a risk-aware culture. (Some firms take integrating a risk-sensitive culture one step further by tying employee compensation to its governance efforts.)

Multiple functional areas collaborate and contribute to the identification and assessment of the company's risks and oversight requirements and actively manage or mitigate those risks. Much more than a passive tracking system of events, ERM allows management to monitor metrics for trends within its business components, understand the firm's status across different functional specialties and jurisdictions in achieving its objectives, and recognize and react to potential issues.

An automated corporate governance tool peels the onion-like layers of the firm's legal entities, organizational authorities, process owners, controls, incidents and their remediation, and audit outcomes to identify themes, trends, and gaps within the organization. Automated and interactive screens and reports allow the user to switch between data aggregation and minute details in any aspect of the legal entity or its processes.

The ERM's firm-wide view offers significant benefits. In life, several risks can occur at the same time; they are not isolated to one business line or functional area. GRC's ability to offer simulations and scenario analysis is helpful here, as is keeping all of the identified risks and historical and current incidents at the user's fingertips. An integrated oversight approach is a more powerful shield than is a fragmented one. Further, in practice, any given risk might be more severe than imagined, so early warning through rigorous review is critical to speedy action.

Keeping identified risks up to date and in sync with the firm's current business objectives and processes is an ongoing effort, and more detail recorded in the system will mean a greater contribution to keeping it current. But a company must use the tool constructively and not become a slave to the tool. Vendors and clients must find the right balance of process mapping that doesn't overload the workflow with too much detail.

Some firms use a top-down implementation and deploy a full ERM system, a complicated process that requires the firm to fully understand all aspects of its business processes. But for many, even large firms, ERM is a complex deployment performed gradually over time, adopting individual modules with an immediate business need, then progressing to other functional areas. The intent is to initiate value where an explicit business need exists, for example in audit or vendor risk management.

MARKET POTENTIAL FOR GRC PLATFORMS

Historically, large financial services firms have used GRC platforms, as they have the financial and staff resources to commit to what has been an expensive, customized platform. Customized platforms require repeat services and fees, often from professional consultancies. But have GRC clients improved efficiencies across governance functions? The answer is yes. Think about all the vast numbers of Excel spreadsheets and other documents in which information is filed. Consider how frequently firms operate in silo mode, with clear and timely communication across segments difficult or nearly impossible.

It's unlikely that GRC solutions can help stop industry meltdowns, but they encourage firms to think about complex processes and potential risks to the firm—external risk and risks from within. They empower firms to develop internal controls and devise risk-mitigation strategies for events that ultimately educate employees. The cumulative effect of planning, tracking, and communicating the GRC content to the firm enables informed minds to take speedier and more meaningful action in the face of an event and in strategic or tactical business decisions. Moreover, a risk-aware corporate culture combined with an organized, methodical approach to GRC deters fraud.

MARKET SIZING

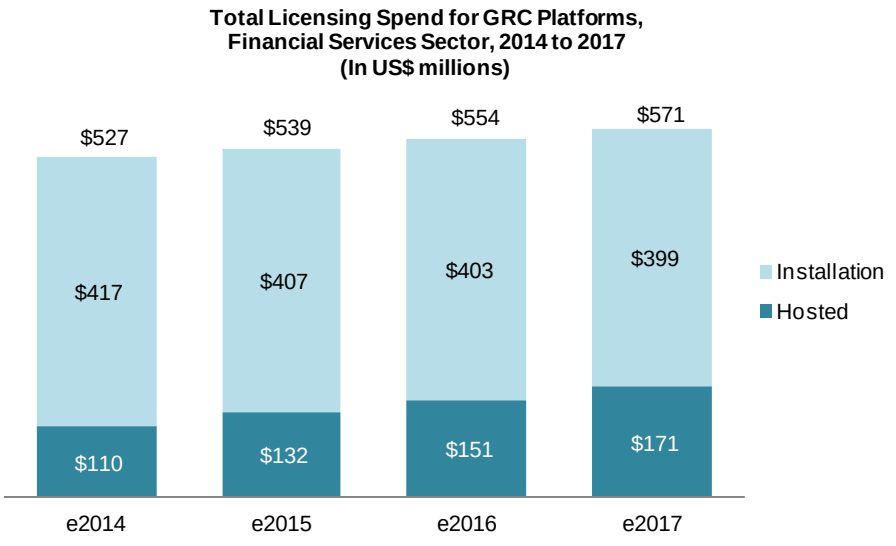
Aite Group anticipates midsize financial services firms will adopt more hosted deployments of GRC platforms, and a few vendors are likely to find their niche in this market. Growth could be higher if vendors further streamline standard deployments and provide the professional services team that nonbank entities—asset managers, for example—can rely on. While client expectations will be high and budgets low, the economy has improved of late.

The regulatory compliance market and governance headlines are a significant incentive for product adoption. Further analytic developments from GRC platforms geared to decision-making, senior executive reporting, and firm collaboration will strengthen GRC platform prospects.

The financial services GRC market shows promise, as vendors consolidate and form larger firms able to support needed solution enhancements, declining prices, and better implementation support and experience. There is a dearth of comprehensive risk and compliance tools on the market and much demand. To date, vendors' new clients have more generally arrived from the existing GRC client population. Clients are jumping ship to capitalize on improvements in other vendors' solutions or gravitating to vendors they believe will provide a better ongoing GRC experience. The audience has begun to broaden and will continue to do so.

The entire GRC market is many billions of dollars in size with market estimates anywhere from US$2 billion to US$10 billion. Further, point solutions in the market cover aspects of GRC or single components of the GRC platform and could be included in such forecasts. Scoping a forecast to include only financial services firms (not financial technology vendors) and only for the wider GRC platform seems the most helpful. GRC platforms' market sizing for the financial services sector is US$527 million in 2014, growing to US$571 million by 2017, an average annual increase of 3.4% (Figure 4). The figures do not include implementation costs.

Figure 4: Licensing Spend for GRC Platforms in Financial Services



Source: Aite Group; figures do not include implementation cost

CAN MY FIRM AFFORD A GRC PLATFORM?

Competition and the availability of a cloud offering have driven down GRC prices for all users. Further, these changes have created options for the midsize market to own a GRC platform. Alongside this benefit, vendors are attempting to provide fast-track implementations with

commonly used frameworks to get firms up and running on GRC. Whether firms will be happy with a standardized product is still undecided.

SOLUTION PRICING STRUCTURE AND OVERALL COST

GRC's pricing structure varies, but vendors generally license the platform and price it according to number of users (there may be a minimum number of users) and number of modules. Most GRC solutions have user profiles that determine the views and content available to a user. Furthermore, permissions may be tied to a tiered pricing structure that separates users who record to the system and users in "read-only" mode (i.e., a "light" user has limited actions, such as an attestation or survey reply). Some vendors will include the number of connection points in the pricing structure.

A number of vendors offer perpetual license fees for on-premises installation with annual maintenance fees that might run 15% to 20% of the license fee. Some vendors provide the hosted deployment for an annual subscription with an additional managed services fee while others charge a single inclusive subscription fee.

As with any system, implementation is a function of the complexity of the client, its business needs, and use of the platform. Vendors' report solution pricing can be less than US$250,000. Complex implementations have the potential to run twice that figure or far more, however, if the solution is customized with the aid of third-party consultants, as a number of asset managers report. The global Big Four consulting firms have an active business supporting financial services firms in implementing and customizing screens and workflow within the GRC solution.

Implementation time frames across solutions generally range from one month to six months. Hosted deployments with standardized implementations are generally shorter, while an ERM use case across a complex organization could take one year (or more, according to some users). Generally, most vendors recommend a well-planned, phased rollout to ensure that the client's staff eagerly adopts the platform. Implementation time frames do not consider situations in which a client decides to build its GRC framework from scratch. This arduous task would begin many months before a vendor would begin the implementation process.

Vendors are pushing to streamline implementation, provide clients with more and varied content, and offer a cloud option, which opens doors to ownership. There's still some way to go to smooth the path for solution implementation. And it would behoove the vendor community to provide more evidence of client benefits via tangible metrics. Overall, the industry will eventually arrive at an easier adoption point with more options.

FULL-TIME RESOURCE COMMITMENTS

While a variety of employees participate in the solution content, the solution requires a champion and overall grandmaster administrator in addition to relevant data feeds. Depending on the scope of solution use, GRC clients may employ one to four people to administer the platform. Administration could include coordinating software upgrades or enhancements, customizing development, modifying structure and content, administering the user base, preparing management reporting, and training staff on the use of the solution.

GRC power users combine skills in IT with an understanding of the firm's business operations. Financial services firms often tap former consultants or individuals who have previous experience with the GRC solution. It is not an easy candidate search, as this individual must also have the personal skills to manage a dramatically varied user base, especially as the solution rolls out to multiple functional areas.

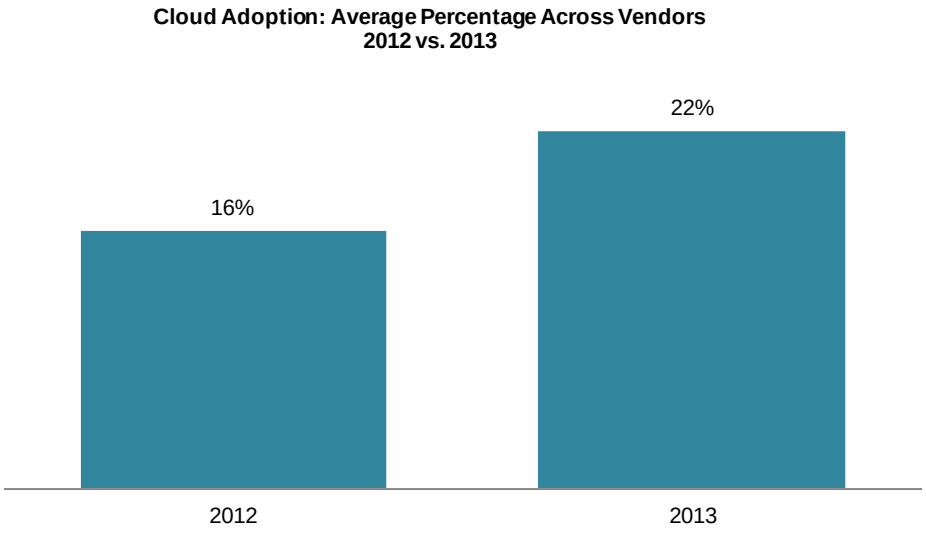
In some cases, clients hire developers dedicated to the GRC platform. This allows for ongoing customizations and may free the firm from the third-party consultants (and their invoices) involved with the original implementation.

CLOUD STATUS

Cloud adoption across all types of clients is slowly rising. Vendors report smaller firms opting for cloud deployment. Adoption may also depend on the use of the system; for example, clients might deploy a hosted version for business continuity matters but prefer an in-house installation to support IT security. Some buyers begin with cloud then shift to an on-premises installation over time.

In terms of firm size, most vendors report new clients or inquiries arising from firms outside of the top 50 financial firms in any particular sector. One vendor reported GRC adoption trending down to small firms in the tens of billions in assets under management. Cloud may well help more firms access the technology. Overall client-base cloud adoption across selected vendors at year-end 2012 was 16% versus 22% in 2013 (Figure 5). MetricStream has one of the highest client populations using a cloud deployment.

Figure 5: Cloud Adoption Makes GRC Available to Wider Community



Source: Aite Group

Vendor use of third-party data centers is rather common today, as cloud offerings are more popular than ever. The big three cloud providers that everybody knows, inside and outside financial services, are Amazon Web Services, Google, and Microsoft Azure, all of which maintain a proprietary, giant network of data centers. GRC vendors have a proprietary data center or utilize one or a mix of third-party data centers for their hosted solutions.

Clients of cloud implementations should always obtain specifics from a vendor relative to the ownership of the data center, the policies and procedures in place around information and physical security, and the availability of statistics and business continuity plans. A financial services firm should also confirm that a third-party data center's contract reflects the same standard of information security protocols the client agreed to with the vendor. Finally, the potential client should inquire about the vendor's ongoing oversight of its subcontractors.

TOP RISKS FOR GRC VENDORS

The GRC client market opportunity is significant, but it does not come without challenges. Vendors and clients note the following:

- **Managing GRC system reputational risk:** Failed and lengthy implementations tarnish a vendor's image and make it more difficult for firms to prove the benefits of the platform. Large-scale ERM implementations can become unwieldy, and resource scheduling for delayed projects can impact other clients.
- **Staffing implementation teams:** Demand for experience in GRC software is increasing, with clients targeting potential candidates as well as the vendors. Demand will heighten as vendors come to realize they need to own (at least as an option) the implementation and professional services market for their products.
- **Reducing solution costs:** Clients find GRC solution costs still high. Upgrades, coupled with third-party custom professional services work, are frequently cited as a pain point for financial services firms. Some circumvent this by hiring staff to perform their own system development work.
- **Keeping up with regulation**: Vendors must keep abreast of an enormous mountain of changes in regulation and industry standards.
- **Staying state-of-the-art:** Client expectations are high regarding upgrades to the platform, architecturally as well as features and functionality. Vendors must address options in cloud deployment, social media, and mobility. Currently, many vendors are focusing on content including data analysis and varied options for GRC frameworks.
- **Coping with a lack of client commitment or traction within its business:** Vendors have experienced difficulty when clients do not assign proper internal resources to support implementation and do not advocate for the GRC project.

- **Navigating a competitive market:** Cloud offerings, pricing declines, and a thinning number of vendors focused on financial services create a challenge for vendors to add greater value more quickly.

VENDOR PROFILE

GRC vendors are slowly gaining momentum in the financial services industry. Vendors are focusing on a discrete area of requirements to meet client objectives and using the strength of their client relationships to expand to other functional areas. The GRC technology market is a competitive one with large, global vendors dominating the field's financial services clients.

METRICSTREAM

COMPANY BACKGROUND

Founded in 1999, MetricStream is headquartered in California with 1,500 employees. The firm's investors include Goldman Sachs, Sageview Capital and Kaiser Permanente Ventures. MetricStream is active in the industry working with leading governance organizations such as the Risk Management Association, Governance, Compliance and Operational Risk, the Securities Industry and Financial Markets Association, and the Professional Risk Managers International Association.

Clients range from the largest and most highly diversified financial organizations to small and midsize financial firms; approximately 40% of clients are from the financial services sector. Sample financial services clients include Federal Home Loan Bank of Chicago, Hudson City Savings Bank, Societe Generale, Whitney Bank and Zurich Insurance Group.

Asset management and insurance businesses are emerging GRC opportunities, along with mid-market banks. In total, the firm has 300 enterprise installations.

GRC PHILOSOPY

MetricStream's GRC vision touches every corner of an organization. Referred to by the vendor as "pervasive GRC," the business vision includes the aggregation of structured and unstructured data, analytics for risk intelligence and contextual analysis, and a collaborative approach for users across the firm and with third parties.

METRICSTREAM PLATFORM

Clients may buy the entire platform or applications to address specific business needs with the AppStudio suite of development tools providing the ability to expand. The solution is available as an on-premise installation or a cloud offering. MetricStream uses third-party, Tier-4 data centers that are SSAE 16 certified.

The platform handles big data—across its varied sources—via an Apache Hadoop DFS-based[5] and Mongo Database framework. The framework supports big-data characteristics and text analytics to identify data patterns and indicators of risk, and it is integrated with MetricStream's

5. Apache Hadoop Distributed File System (DFS) is an open-source software framework for storage and large-scale processing of data-sets on clusters of commodity hardware.

ERM framework. The vendor's goal is to tap content for risk intelligence that will help drive the client's growth and performance. As an example, MetricStream is working with financial services clients to aggregate end-client feedback on their financial-product portfolio from multiple sources including social media and other open sources. This could proactively highlight the conduct risk and governance-related issues pertaining to the vendors' marketing and selling practices for the client.

MetricStream has a library of standards and frameworks from authoritative sources that clients may customize, or they can upload their own. MetricStream features out-of-the-box regulatory libraries from more than 25 regulators from more than 17 countries. Workflow tools support task assignments, approval processes, and action alerts. The solution also supports historical look-backs in time for audit purposes.

The graphic user interface is intuitive and clear and supports sophisticated data visualizations, simulations, analytics, and interactive dashboards. Charts include interconnection maps, heat maps, Gantt charts, histograms, pie charts, and Excel-compatible charts and graphs. The system has more than 155 standard reports and supports additional user report creation via a simple report wizard. Users may create executive-style dashboards. Production reports are done in Jaspersoft Business Intelligence Software.

MOBILITY AND AN APP MARKET

The vendor created Zaplet.com, a cloud-based development environment with the AppStudio suite of development tools. The Zaplet framework allows business partners to perform the entire application-creation life cycle in the cloud, from development to deployment, for their unique requirements. The GRC app store allows business partners to easily create and share content, which extends the features of MetricStream's GRC platform. Business partners have developed apps to serve up legal and regulatory content, perform calculations related to a specific investment instrument, or address a particular process requirement.

SOLUTION MODULES

The GRC platform is frequently sold as a single platform with multiple applications that clients may turn on and off or add separately (Table A).

Table A: Core Platform Components

Vendor	Description
MetricStream	A single platform with all components installed with the first module deployment. Key product modules include: 1. Enterprise Risk Management 2. Operational Risk Management 3. Compliance Management 4. Regulatory Change Management 5. Audit Management 6. SOX Compliance Management 7. IT Risk Management 8. IT Compliance Management 9. Threat and Vulnerability Management 10. Business Continuity Management

Vendor	Description
	11. Incident Management 12. Policy and Document Management 13. Case Management 14. Vendor Risk Management 15. Scenario Analysis

Source: MetricStream

SIMPLIFY GRC

MetricStream's goal is to simplify GRC. This intention begins with the selling process and product selection and flows through to specification development and implementation. As with any core technology, the more pervasive the use of the GRC platform across the organization, the greater its validation and usefulness within the firm.

Beyond implementation, MetricStream strives to provide ongoing support to the GRC program overall. The firm maintains an educational platform, MetricStream University, with training, workbooks, and client workshops as well as ongoing client service support.

The firm designed a FastTrack implementation in support of less complex client environments. MetricStream also advocates gradual module adoption and can meet immediate client requirements while allowing time for the client organization to adapt to an enterprise GRC framework.

For years, financial institutions have had difficulty furthering solution adoption due to difficult and delayed implementations, complex frameworks, expensive modifications, and a lack of broad adoption within the firm.

MetricStream's mission to simplify GRC is driven by three concepts to embed GRC use within the firm:

- **Adoption** seeks to engage users to participate in GRC requirements. These features recognize the modern business environment, supporting, for example, multiple devices in a mobile world, an intuitive graphical user interface alleviating the need for a help menu, and contemporary collaborative features such as (internal) social networking interactions. Thinking outside of the box, one adoption tool is a reward-driven feature taken from training environments that acknowledges correct answers, tasks, or behaviors consistent with firm requirements or desired outcomes.

- **Layering** acknowledges the business reality of bidirectionally linked business-process systems and the necessity of connectivity in today's financial institution. MetricStream acknowledges the need for an open system using open APIs to support extended cloud architectures with third-party systems and information services. The firm is extending this effort and seeking to develop an ecosystem for the GRC environment by lining up various technology, information services, analytics, and/or visualization systems to facilitate client access to needed resources. This ecosystem recognizes the existence of multiple GRC platforms or components in

a large complex financial institution with the ability to intelligently aggregate details for enterprise reporting.

- **Contextualization** is supported by allowing user configurability through the Zaplet marketplace, integrating GRC intelligence for content such as social media and news, and using a federated data model that understands the complexity of big data and its existence across the organization.

Unlike point technology systems that perform discrete functions within a client firm, the GRC platform depends on collaboration and direct contribution from multiple functional areas. Added to this challenge, the GRC platform and financial technology in general is evolving during one of the most seismic shifts in regulatory compliance in decades and a period of new unknowns in enterprise risk management that encompass geopolitical, economic, market, and business risks. In a challenging and competitive market, vendors must do more than provide a technology platform. Client success relies on vendors as an authentic partner in an ecosystem of vendors and business requirements.

CONCLUSION

It is not possible to foresee every turn on the road, but educated, prepared staff can adjust their actions more quickly as the road turns. As William Arthur Ward once said, “The pessimist complains about the wind; the optimist expects it to change; the realist adjusts the sails.”

GRC platforms are a tremendous help in centralizing information in a repository of official documents, furthering collaboration and communication among teams, and easily demonstrating the interconnectivity of business processes, controls, risks, incidents, regulatory impact, and action plans.

The software is gradually moving in the direction of big data and analytics, seeking to provide actionable insights to the firm’s activities and experience.

GRC platform users are still looking for improvements, however, such as the following:

- Varied and flexible prebuilt framework libraries and content to speed implementations
- Ideas and means to lower the high-touch data entry needs, more connectivity, and automated workflow
- The ability to lower the use of or eliminate the dependency on expensive third-party consultants
- Flexible solutions that will “hear the voice” of multiple firm divisions
- User-controlled ad hoc reporting to elevate analysis; for example, visualizations that provide compact yet aesthetic presentations of data

The various types of financial services firms—asset managers, hedge funds, insurance companies, asset servicers, and banks—all have their own languages, menus of products, operations, and unique workflows. Certainly, it is a challenge to tackle all financial services industry needs. After all, GRCs are still young by core infrastructure software standards. Yet in the financial services industry’s new era, there is opportunity to grow the solution, mature the target market, and improve the adoption rate.

The last several years have been one rocky boat for the financial services industry. Although there’s no shortage of rough seas across all industries, our expectations for those that manage our financial well-being are high. While our captains steer the new course, every one of us is a sailor and must apply our new skills and keep a watchful eye on the industry.

ABOUT

METRICSTREAM

MetricStream is a market leader in enterprise-wide Governance, Risk, Compliance (GRC) and Quality Management Solutions. MetricStream solutions are used by leading global corporations in diverse industries such as Financial Services, Healthcare, Life Sciences, Energy and Utilities, Food, Retail, CPG, Government, Hi-tech and Manufacturing to manage their risk management programs, quality management processes, regulatory and industry-mandated compliance and other corporate governance initiatives. MetricStream's customers include Procter & Gamble, UBS, Societe Generale, Pfizer, Philips, Cummins, Kellogg's, Mondelez International, SanDisk, and NetApp. MetricStream also owns and operates the www.ComplianceOnline.com portal, the largest GRC advisory network and one of the largest GRC communities. MetricStream is headquartered in Palo Alto, California, USA (www.metricstream.com).

AITE GROUP

Aite Group is an independent research and advisory firm focused on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, securities & investments, and insurance, Aite Group's analysts deliver comprehensive, actionable advice to key market participants in financial services. Headquartered in Boston with a presence in Chicago, New York, San Francisco, London, and Milan, Aite Group works with its clients as a partner, advisor, and catalyst, challenging their basic assumptions and ensuring they remain at the forefront of industry trends.

AUTHOR INFORMATION

Denise Valentine
+1.618.398.5061
dvalentine@aitegroup.com

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com
For all press and conference inquiries, please contact:

Aite Group PR
+44.(0)207.092.8137
pr@aitegroup.com