



Corporate Integrity, LLC

Strategic Direction in Governance, Risk, & Compliance

GRC.Perspectives Research

2008 GRC Drivers, Trends, & Market Directions

April 2008

*Are you an organization looking to
implement a GRC strategy or purchase GRC
products, services, or content?*

Corporate Integrity, LLC offers
complimentary inquiry consultations via
email or phone to assist organizations in their
GRC strategy and purchase decisions.

Prepared By: **Michael Rasmussen**
President

Corporate Integrity, LLC
research@Corp-Integrity.com
www.Corp-Integrity.com

Executive Summary

The Governance, Risk, and Compliance (GRC) market is in significant momentum as organizations embrace collaboration across silos of GRC and generally recognize that something needs to be done. GRC is more than a catchy acronym used by technology providers and consultants to market their solutions – it is a philosophy of business. This philosophy permeates the organization - its oversight, its processes, and its culture. The organization goes beyond “talking its talk” to demonstrating that it “walks its talk.” Organizations are driven to ‘think’ GRC. The complexity of business, increasing risk and regulatory profiles, as well as the nature of extended and global business requires that organizations reengineer how they approach governance, risk, and compliance by leveraging processes as GRC. Corporate Integrity sizes the GRC market in 2008 at approximately \$52.1 billion. This is broken down into the three primary categories of Corporate Integrity’s **GRC.EcoSystem** – GRC professional services, GRC technology providers, and GRC information/content providers.

Table of Contents

ORGANIZATIONS EMBRACE GRC PRINCIPLES	3
GRC IS ABOUT ORGANIZATIONAL COLLABORATION	3
DRIVERS INFLUENCING CORPORATE DIRECTIONS IN GRC	5
SILOS OF GRC LEAD TO GREATER EXPOSURE TO RISK	6
2008 TRENDS MATURING GRC PRACTICES	8
THE GRC MARKET IN MOMENTUM	11
UPCOMING GRC.PERSPECTIVES RESEARCH	13
ABOUT THE AUTHOR	14
MICHAEL RASMUSSEN, PRESIDENT	14
CORPORATE INTEGRITY, LLC	15

© 2008, Corporate Integrity, LLC. All rights reserved.

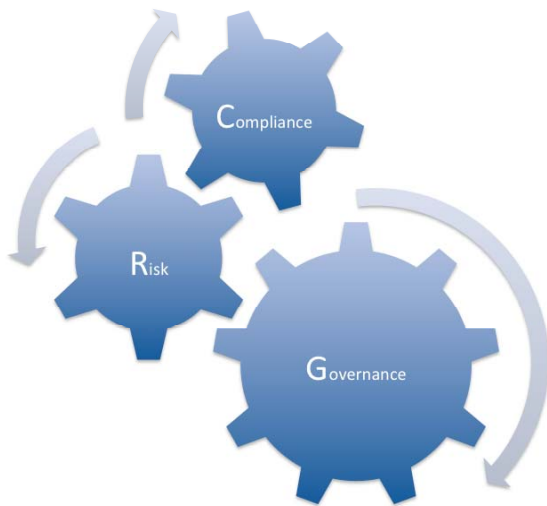
This research is for the exclusive use of the organization which purchased it and is not to be shared outside the organization without permission. Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com

Organizations Embrace GRC Principles

The Governance, Risk, and Compliance (GRC) market is in significant momentum as organizations embrace collaboration across silos of GRC and generally recognize that something needs to be done. However, defining GRC can be difficult, is often misunderstood, and organizations struggle to grasp where to start.

The following standard definitions are used to define the components of GRC:



- **Governance** is the culture, policies, processes, laws, and institutions that define the structure by which companies are directed and managed.ⁱ
- **Risk** is the effect of uncertainty on business objectives; risk management is the coordinated activities to direct and control an organization to recognize opportunities while managing negative events.ⁱⁱ
- **Compliance** is the act of adhering to, and demonstrating adherence to, external laws and regulations as well as corporate policies, procedures, and controls.ⁱⁱⁱ

GRC is About Organizational Collaboration

GRC is more than a catchy acronym used by technology providers and consultants to market their solutions – it is a philosophy of business. This philosophy permeates the organization - its oversight, its processes, and its culture. It is about individual GRC roles across the organization working in harmony to create a collaborative environment for governance, risk, and compliance. It is about collaboration and sharing of information, assessments, metrics, risks, investigations, and losses across these professional roles. It is also about reducing uncertainty in business and producing predictable results.

Organizations are approaching GRC to get an enterprise view of risk and compliance with a specific need to identify interrelationships in today's complex and distributed business environment. This requires that GRC initiatives involve a federation of professional roles – the corporate secretary, legal, risk, audit, compliance, IT, ethics, corporate social responsibility, finance, quality, environmental, health and safety, line of business, and others – working together in a common framework, collaboration, and architecture to achieve:

© 2008, Corporate Integrity, LLC. All rights reserved.

This research is for the exclusive use of the organization which purchased it and is not to be shared outside the organization without permission. Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com

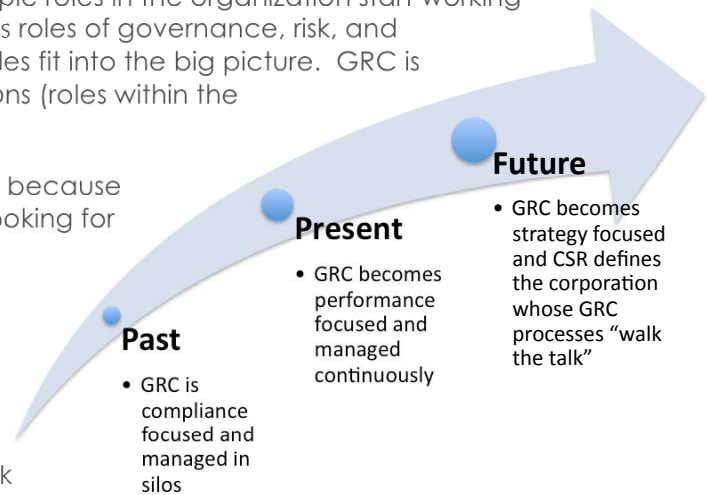
■ **Sustainability.** Organizations demand a sustainable process and infrastructure for ongoing governance, risk, and compliance processes that are becoming more onerous. Further, organizations need to sustain their risk and compliance management practices on a continuous basis: as business is changing rapidly – point in time assessments are no longer good enough by themselves. Business is changing hour-by-hour and minute-by-minute. The dynamic nature of business demands that an organization address GRC collaboratively and continuously.

■ **Consistency.** Organizations require that multiple roles in the organization start working together in an integrated framework. Business roles of governance, risk, and compliance need to understand how their roles fit into the big picture. GRC is getting everyone to play their different positions (roles within the enterprise) out of the same playbook.

■ **Efficiency.** The line-of-business is fighting back because redundant assessment and audit processes looking for similar information for different purposes is preventing the business from getting business done. GRC aims to ease the burden on business by leveraging common processes, assessments, and information.

■ **Transparency.** Business demands transparency across key-performance and risk

indicators so it can monitor the organization's health, take advantage of opportunity, and avert or mitigate disaster. Corporate performance management is tightly related to risk management. When done correctly performance and risk management are two sides of the same coin.



As a result, GRC is moving from the '*past*' of individual silos working autonomously, to the '*present*' where GRC is becoming collaborative and focused on aligning with business performance, to the '*future*' where GRC integrates with Corporate Social Responsibility (CSR) to demonstrate that an organization is an organization of integrity. The organization goes beyond “talking its talk” to demonstrating that it “walks its talk.”

Drivers Influencing Corporate Directions in GRC

GRC is a three-legged stool: governance, risk, and compliance are each individually necessary components for effectively managing and directing an organization. In summary - good governance is built upon diligent risk and compliance management processes.

In today's business environment, ignoring a federated^{iv} view of GRC results in business processes, partners, employees, and systems that behave like leaves blowing in the wind. GRC aligns them to be more efficient and manageable. Inefficiencies, errors, and potential risks can be identified, averted, or contained. This reduces the risk exposure of the organization and creates better business performance. Organizations face a complex array of risk and compliance demands impacting business. The more extended and distributed the business - the more challenging risk and compliance is to manage.

Through ongoing research and interactions with organizations around the world, Corporate Integrity has identified the following drivers that are the primary influencers driving organizations to consider and adopt GRC strategies:

- **Growth of Corporate Social Responsibility.** Organizations are focused on environmental, financial, and social aspects of corporate governance brought together under the umbrella of Corporate Social Responsibility (CSR). Nearly all of the Global 100 have published CSR reports, and a significant portion of the Global 1000 have done so. GRC is intersecting with CSR initiatives as organizations seek to validate the reality of their CSR practices within the organization. Compliance to laws and regulations, avoiding mishaps and events, and managing risk within defined limits all impact an organization's CSR practices and statements of accountability. Further, stakeholders and investors are becoming increasingly conscious CSR issues, choosing to invest in socially responsible organizations.^v
- **Increasing governance demands.** The Board of Directors is rolling up their sleeves and becoming more involved as directors face personal risk within their roles. Beyond Sarbanes-Oxley, organizations are weary of increased regulatory actions, risk inherent in a highly competitive global environment, corporate litigation, as well as stakeholder/shareholder retaliation.
- **Rating agencies focused on enterprise risk management.** Corporate credit rating agencies are focused on evaluating corporate understanding, management, and response to enterprise risk. Enterprise Risk Management (ERM) now has an impact on the organization corporate credit rating. This is forcing many board and executive discussions on strategies for approaching ERM.^{vi}
- **Increasing risk profile in a distributed world.** Business is dynamic and global. As organizations expand operations, their risk profile has grows exponentially. Organizations today have to monitor risk to their business internally (e.g., their internal controls and processes) and externally (e.g., the competitive, legal, and geographic environments) to stay competitive in today's market. To succeed in global business requires that organizations be keenly aware of global financial markets,

© 2008, Corporate Integrity, LLC. All rights reserved.

This research is for the exclusive use of the organization which purchased it and is not to be shared outside the organization without permission. Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com

economic directions, environmental issues, global supply chains, varying regulatory practices, and more.

- **Connecting performance management to risk management.** Companies are discovering that in order to manage corporate performance they also need to manage risk. For every key-performance indicator defined to meet strategic objectives there are several corresponding key-risk indicators to monitor which impact the uncertainty of hitting those objectives.
- **Increasing regulatory compliance profile.** Regulatory compliance is a key topic of discussion from the top of the organization down into the trenches of business operations. Executives have become all too familiar with terms such as *consent decrees*, *deferred prosecutions*, and *corporate integrity agreements*. Organizations face expanding regulations, increased fines & sanctions, and aggressive regulators and prosecutors around the world.^{vii} There is also a global trend to move regulatory oversight to a principle-based regulations.^{viii}
- **Impact of the extended enterprise.** Today's business is not a self-contained entity but a complex web of business relationships. Factoring in expanding regulations, increasing litigation, growing risk profile with the dynamic (changing) and distributed business – the demands for a strategic approach to GRC is clear. Organizations need to validate that the extended enterprise (e.g., business partnerships, contractors, consultants, outsourcers, suppliers) is complying with laws, meeting their social responsibility practices, and not introducing unnecessary risk.



Source: Open Compliance & Ethics Group

- **Inefficient, manual, and siloed risk and compliance initiatives are ineffective.** Islands of risk and compliance that operate autonomously introduce further risk in today's complex and distributed business environment. Organizations require an enterprise view of GRC that brings together the silos of risk and compliance. What may seem like an insignificant risk in one part of the organization may very well have a different appearance when other risks are factored into its relationship and impact.^{ix} Organizations face out-of-sync controls and corporate policies that are inadequate to manage risk and compliance. Further, executives are becoming aware of redundant risk and compliance projects from different parts of the organizations wasting company time and resources with manual and laborious assessments that fail to leverage technology and information.

Silos of GRC Lead to Greater Exposure to Risk

A reactive and siloed approach to GRC is a recipe for disaster and leads to . . .

© 2008, Corporate Integrity, LLC. All rights reserved.

This research is for the exclusive use of the organization which purchased it and is not to be shared outside the organization without permission. Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com

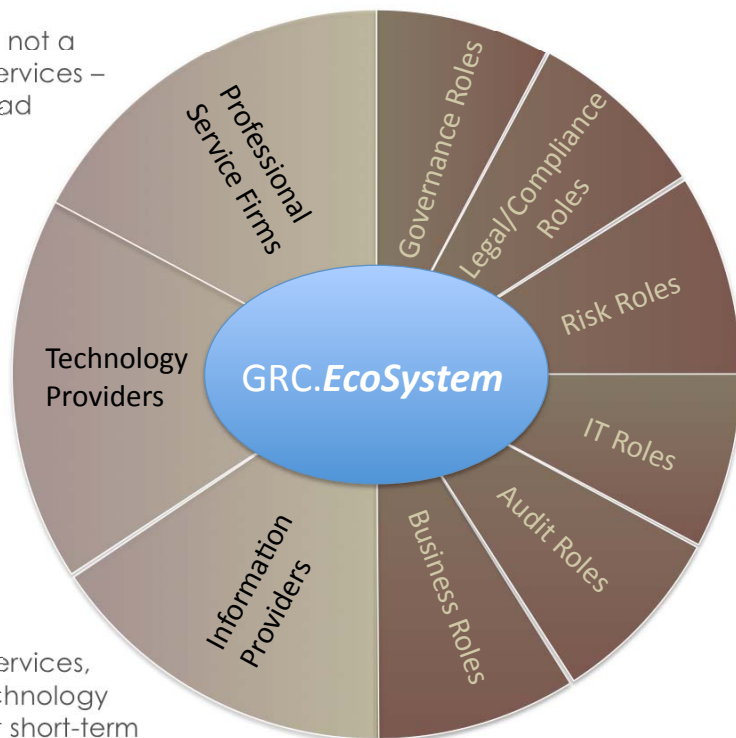
- **Lack of visibility.** A reactive approach to risk and compliance leads to siloed initiatives that never see the big picture. No one was thinking how controls could be architected to meet a range of compliance needs. This results in poor visibility across the organization and its control environment, as there is no framework or architecture for managing risk and compliance holistically.
- **Wasted and/or inefficient use of resources.** Silos of risk and compliance lead to wasted resources. Instead of thinking of the big picture and how resources can be leveraged to meet a range of risk and compliance needs, they are instead developed independently. The organization ends up with varying processes, systems, controls, and technologies to meet individual risk and compliance requirements. Many of these processes and controls could have been streamlined with a common framework approach to GRC.
- **Unnecessary complexity.** Varying risk and compliance approaches introduce greater complexity to the business environment. With complexity comes an increase of inherent risk. Complexity means that controls are not streamlined and managed consistently introducing more points of control failure, compliance gaps, and unacceptable risk. Inconsistency in controls means inconsistency in documentation of compliance that can further confuse the organization, regulators, and business partners.
- **Lack of flexibility.** Complexity drives inflexibility - the organization is not agile to the dynamic business environment it operates in. The organization becomes so wrapped up in spinning several risk and compliance plates that business performance is degraded. Business becomes bewildered in a maze of varying approaches and control requirements that have fail to be addressed with any sense of consistency or logic.
- **Vulnerability and exposure.** A reactive approach leads to greater exposure and vulnerability. This is a further fruit of complexity – everyone is focused on his or her silo of risk or compliance. No one sees the big picture. No one is looking at controls holistically. The focus is on what is immediately before them and not what the business needs to protect itself in the long run. Additionally, varying and independent efforts of risk and compliance lead to a difficult process of demonstrating enforcement and audit compliance. It also leads to duplication and gaps in coverage and a workforce that is ill equipped for success.

2008 Trends Maturing GRC Practices

Organizations are driven to 'think' GRC. The complexity of business, increasing risk and regulatory profiles, as well as the nature of extended and global business requires that organizations reengineer how they approach governance, risk, and compliance by leveraging processes as GRC.

The 2008 GRC trends within global enterprises addressing GRC include:

- GRC 2.0 – the GRC.EcoSystem.** There is not a one-stop shop for GRC products and services – no one vendor has it all. GRC in its broad sense impacts a range of consulting professions as well as a range of technology issues. GRC 1.0, which Michael Rasmussen of Corporate Integrity was the first to define, typically was about a coordinated response to issues such as Sarbanes-Oxley and IT risk/controls. GRC 2.0 is about re-architecting business processes and systems to provide a complete 360-degree view of governance, risk and compliance across business areas in the enterprise. This requires that organizations gain a solid vision for the expanse of GRC activities within their corporation and understand the range of professional services, information/content providers, and technology solutions that can bring success to their short-term and long-term GRC strategies.



- Maturation of GRC technology.** In response to the principles behind GRC 2.0, organizations are demanding that technology vendors marketing GRC play well with each other. Integration has become critical as GRC platforms need to tie into enterprise applications and infrastructure as well as play well with other GRC related applications. Organizations are embracing technology to get away from document centric approaches to GRC that are based on paper, electronic documents, and spreadsheets. The current demand is for platforms with advanced content and process management capabilities. Technology growth directions for the next several years include advanced risk analytics/modeling, automated controls tied to business rules engines, and embedded GRC control points.

© 2008, Corporate Integrity, LLC. All rights reserved.

This research is for the exclusive use of the organization which purchased it and is not to be shared outside the organization without permission. Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com

- **Next generation policy and procedure management.** A significant area of business demanding an overhaul is how organizations manage policies and procedures. The past has burdened business with policy manuals on office shelves and an array of Intranet websites with published policies that tend to be out of date and never read. This goes contrary to current regulatory/legal pressures that require an organization to defend itself by demonstrating that individuals knew the policy, attested to their behavior, and were trained on it. This problem grows with the extended enterprise when business partners, contractors, consultants, and even temporary workers need to read, understand, be trained, and acknowledge behavior to corporate policies and procedures. These demands on policy and procedure management are causing organizations to consider new approaches to manage the policy and procedure lifecycle – definition, approval, distribution, communication, training, attestation, accessibility maintenance, and retention.
- **Enterprise investigations and loss management.** In addition to policies and procedures, organizations are handicapped in their risk strategies when they have no view into enterprise losses and investigations. Organizations typically do not document loss – and have inconsistent approaches for managing investigations, issues, events, and complaints. When they are managing these areas they, tend to be trapped in silos of home grown spreadsheets and personal databases. Facing an increased risk profile, regulatory environment, and the growth in corporate litigation, organizations have discovered they need to get a better grasp on managing investigations and losses across the organization. This requires the implementation of an enterprise investigation and loss management platform into which the varying roles of GRC can plug into. Those looking at developing ERM strategies are finding they must get a handle on loss, as it is a key factor used to measure and model risk.
- **Policing the extended enterprise.** The distributed nature of business with an interconnected web of business relationships is causing GRC headaches. Organizations have a growing awareness that business partners, contractors, consultants, and temporary workers need to attest to policies and be trained. Further, organizations typically have a range of business relationships that they cannot assess and monitor compliance to contracts and regulations. Each relationship typically has a contract with a right-to-audit clause in place, but the organization lacks the personnel to exercise right-to-audit clauses. Organizations are beginning to revamp how they manage risk, compliance, and controls in the extended enterprise – which leads to the following trends . . .
- **Software as a Service grows as a GRC implementation model.** GRC Software as a Service (SaaS) solutions have had historical success within small to medium-sized companies trying to manage risk and compliance as well as with large companies that need to do it very quickly. However, Corporate Integrity is now seeing growth in the GRC market that provides Software as a Service (SaaS) solutions to large and distributed enterprises to meet the needs of communicating policies and conducting risk/control assessments to the extended enterprise. SaaS allows the organization to communicate policies and push self-assessments out to business partners without opening up holes into its own internal network and systems. Currently, over one-third of GRC deals are awarded to SaaS GRC vendors – and Corporate Integrity expects that number to grow. SaaS for GRC is an excellent way to respond to regulators and prosecutors when the need to react quickly to issues in the environment (e.g., communicating policies) arises and there is no time for a large IT project. It also allows organizations to develop a prototype and prove the benefits of a collaborative platform

© 2008, Corporate Integrity, LLC. All rights reserved.

This research is for the exclusive use of the organization which purchased it and is not to be shared outside the organization without permission. Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com

for GRC in the enterprise without a significant impact on infrastructure, people, and resources. SaaS is also plain and simply a cost-effective way to get a GRC model moving quickly within an organization.

- **Beginning of GRC outsourcing.** Organizations have embraced an array of business process and IT outsourcing – the next is outsourcing of GRC processes. Number one on the agenda is the outsourcing of risk and compliance assessments of extended enterprise. Corporate Integrity is seeing this currently in the supply chain risk management space. Faced with global trade compliance -- product recalls; operational risk to manufacturing, distribution and retail; as well as geo-political risk that spans business operations around the globe – organizations are beginning to look to external partners that can assess and monitor the risk within their supply chains on an ongoing basis.
- **Risk & regulatory intelligence.** Information is key to managing risk and maintaining compliance. To stay informed of a dynamic risk and regulatory environment across geographies and legal jurisdictions, organizations are looking to information and content providers to inform them of changing risk, regulatory, and legal conditions that impact their business. From a risk perspective, organizations want to monitor global risks to their business such as foreign exchange, economic conditions, civil unrest, terrorism, environmental/weather alerts, and local political concerns. The regulatory perspective requires that organizations stay abreast of new or changing regulations, case law, and enforcement actions. Further, organizations are looking to be informed of new and pending legislation that impacts their business. This requires that organizations develop skills and processes internally to monitor GRC activities as well as hook their GRC systems into external information/content providers.
- **GRC is growing organically within organizations.** Five years ago, when Michael Rasmussen first defined and modeled the GRC market, organizations wanted solutions focused on a single silo of risk or compliance. They were concerned about addressing SOX, Basel II, HIPAA, employment/labor compliance, global trade and not looking across the enterprise for similar requirements. Today's GRC deals tend to be multi-domain or enterprise in scope. Although organizations are not starting out to swallow the ocean – they are focused on key issues but want something that can be leveraged in other areas as GRC expands organically within the organization.
- **GRC is spanning industry verticals and business processes.** Corporate Integrity is monitoring GRC activities across industries. Historically, financial services and life sciences have received the most GRC attention. From a business process perspective SOX has been the greatest GRC focus of the past several years. Today Corporate Integrity is seeing strong interest in GRC from several industry verticals and business process domains. There is significant interest in GRC within airlines, energy, utilities, manufacturing, and retail; which have outsourced operations and extended business relationships. These firms have realized that operational quality and compliance is becoming a risk to the franchise. Recent airline fiascos, NERC fines due to poor operational quality, toy recalls, and environmental concerns are driving GRC adoption across industries.

The GRC Market in Momentum

The GRC market is growing and expanding - though, from a market size perspective, it remains difficult to define and put boundaries around. Sizing the GRC market is a challenging task as GRC market boundaries are difficult to define – arguments can be made for broader or tighter definitions.

Corporate Integrity sizes the GRC market in 2008 at approximately \$52.1 billion. This is broken down into the three primary categories of Corporate Integrity's **GRC.EcoSystem**:

- **GRC Professional Service Market is \$40.6 billion in 2008.** The professional service market for GRC represents the majority of the GRC spending as organizations leverage consultants, auditors, and lawyers regularly to provide assessments of risk and compliance. The professional service market also encompasses the array of system integrators and outsourcers positioning GRC in their service portfolios as well.

Corporate Integrity tracks roughly 200 professional service firms offering services related to GRC –the Big 4 audit firms representing the bulk of this market.

- **GRC Technology Provider Market is \$9.3 billion in 2008.** The technology provider market for GRC is shifting significantly. The bulk of the market is represented by hundreds of software vendors that are under \$20 million in revenue while the enterprise application/ERP vendors are starting to gain momentum on delivering products within their GRC strategies. Corporate Integrity currently tracks approximately 600 technology providers that play in the GRC market space. The majority of these vendors span specialty risk and compliance areas – AML, global trade/OFAC compliance, SOX, quality, EH&S, and other GRC sub-domains. Much of this market is moving toward consolidation as large vendors aim to expand their portfolio of GRC technology offerings and capabilities.

At the core of this market are GRC Management platforms that provide content and process management capabilities that assist organizations in: policy and procedure management, risk and control assessment, loss & investigations management, and GRC modeling and analytics. There are 115 vendors focused on delivering this core GRC management platform and the 2008 market size for this segment is \$1.1 billion.

- **GRC Information/Content Provider Market is \$2.2 billion in 2008.** The information/content provider market for GRC is the most difficult to define and model. It represents an array of companies that offer solutions to inform organizations of changing risk and regulatory conditions. Legal research providers encompass much of this market size. Corporate Integrity is currently monitoring fewer than 50 providers in this market.

The boundaries of the GRC market can be expanded or contracted depending on definition and scope. Corporate Integrity's figures do not include some significant market areas of GRC that could be argued should be included. The security market is one example of a market segment that is easily defined as part of GRC but is not completely included in Corporate Integrity's sizing as it is a complete market segment within itself.^x

© 2008, Corporate Integrity, LLC. All rights reserved.

This research is for the exclusive use of the organization which purchased it and is not to be shared outside the organization without permission. Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com

Overall the GRC market has grown significantly over the past five years since its original formation out of the wake of Sarbanes-Oxley. As more vendors have turned their marketing messaging to use the term GRC – and the definition of the market has expanded – it is difficult to state how much it has grown without getting into specific sectors of the **GRC.EcoSystem** where accurate comparisons can be made.

Corporate Integrity expects 15% growth in the GRC market over the next 18 months. 2009 should bring an aggregate GRC market figure size nearing \$50 billion. Most of the growth in the GRC market remains within organizations tackling hot and pressing GRC issues with a goal to leverage what they are doing for other GRC purposes down the road. Even organizations with broad GRC visions are learning they have to start in a few areas and let it grow organically.

Upcoming GRC.Perspectives Research

Corporate Integrity, LLC is working on the following upcoming research pieces in the GRC space:

- *Strategies for Enterprise Investigations Management*, April 2008
- *GRC 2.0 - The GRC.EcoSystem*, May 2008
- *Developing a GRC Strategy and Framework*, June 2008
- *Next Generation Policy & Procedure Management*, July 2008
- *Developing a Regulatory Intelligence Strategy*, August 2008
- *Marketing Corporate Compliance: Success Strategies in Branding Your Corporate Compliance Program*, September 2008
- *Developing a Risk Intelligence Strategy*, October 2008
- *Monitoring Risk with Risk Dashboards*, November 2008
- *Effectively Managing Geo-Political Risk*, December 2008

© 2008, Corporate Integrity, LLC. All rights reserved.

This research is for the exclusive use of the organization which purchased it and is not to be shared outside the organization without permission. Reproduction in any form is strictly prohibited without express permission. For reproduction rights, usage information, and to purchase reprints contact: research@Corp-Integrity.com. Information is based on best available resources. Opinions represent judgment at the time and are subject to change.

www.Corp-Integrity.com

About the Author



Michael Rasmussen, President

Michael Rasmussen is the authority in understanding Governance, Risk, and Compliance (GRC). He is a sought after keynote speaker, author, and collaborator on GRC issues around the world and is noted for being the first analyst to define and model the GRC market for technology and professional services.

With more than 15 years of experience, Michael's objective is to assist organizations in defining GRC processes that are sustainable, consistent, efficient, and transparent. His thought leadership is tuned to:

- Educate GRC professionals within corporations to identify, understand, and analyze GRC strategies, drivers, trends, and best practices;
- Assist technology providers with alignment of their product and marketing strategies to the needs and requirements of GRC professionals; and
- Collaborate with professional service firms on their portfolio of GRC service offerings to better equip them to serve their respective clients.

A leader in understanding risk and compliance standards, frameworks, regulations, and legislation, Michael aims to improve corporate integrity through advancing GRC initiatives. He has served in leading roles in public policy contributions to US Congressional reports and committees, interacted with organizations around the world on GRC, and currently serves on the Leadership Council and Steering Committee of the Open Compliance and Ethics Group. Michael has been quoted extensively in the press and is respected for his commentary on broadcast news channels.

In June 2007, *Treasury & Risk* recognized Michael as one of the 100 most influential people in finance with specific accolades noting his work in "*Governance and Compliance: Saving the Planet and the Corporation.*"

Michael can be contacted at:

+1.888.365.4563 (office)

mrasmussen@corp-integrity.com (email)

<http://blog.corp-integrity.com> (blog)

Corporate Integrity, LLC

Corporate Integrity, LLC is a strategy & research advisory firm providing education, research, and analysis on enterprise governance, risk management, and compliance.

Through ongoing research, interactions, and analytics, Corporate Integrity is the authority in understanding how organizations can foster a culture that “walks the talk” – where integrity is central to governance, risk and compliance (GRC) practices. Corporate Integrity educates organizations and GRC professionals within those organizations on achieving sustainability, consistency, efficiency, and transparency in their corporate GRC practices to maintain a position of integrity aligned with corporate values and business performance.

In addition to helping organizations understand and improve their internal GRC processes, Corporate Integrity assists technology providers and professional service firms in aligning their sales, product, service, and marketing strategies to the requirements of the roles responsible for GRC.

With the deepest GRC expertise and understanding available in the market, Corporate Integrity has developed a range of service offerings to assist organizations, GRC professionals, technology vendors, and professional services firms focused on GRC.

Corporate Integrity, LLC

Tel: +1.888.365.4560

Fax: +1.888.365.4561

Email: research@Corp-Integrity.com

www.Corp-Integrity.com

Thank you for supporting Corporate Integrity's research by purchasing this document. For hard-copy or electronic reprint rights, contact Corporate Integrity research staff at +1.888.365.4560 or research@Corp-Integrity.com.

Please send feedback or ideas to research@Corp-Integrity.com!

ⁱ The Organization for Economic Cooperation and Development (<http://www.oecd.org>) has done significant work on promoting the concepts of this definition in their principles of corporate governance. http://www.oecd.org/document/49/0,3343,en_2649_37439_31530865_1_1_1_37439,00.html

ⁱⁱ This definition of risk is modified slightly from the AS/NZS 4360:2004 risk management standard (<http://www.riskmanagement.com.au/>). This standard is also the basis for a new ISO risk management standard in development to be released later in 2008. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43170

ⁱⁱⁱ The principles and structure of this definition are relevant in much of the excellent work that the Open Compliance and Ethics Group (<http://www.oceg.org>) has done.

^{iv} A federated approach is one in which independent areas of the organizations work together under a common framework.

^v The World Business Council for Sustainable Development defines Corporate Social Responsibility as “. . . the continuing commitment by business to behave ethically and contribute to economic development while improving the quality of life of the work force and their families as well as of the local community and society at large.”

^{vi} Standard and Poors has been the most aggressive in pursuing ERM as a component of determining corporate credit ratings. <http://www2.standardandpoors.com/portal/site/sp/en/us/page.article/3,1,1,0,1148450713660.html>

^{vii} The regulatory environment burden is not getting any easier. *The Wall Street Journal* reported on the increased regulatory environment within the current state of politics – Monday, March 24, 2008 *“Political Pendulum Swings Toward Stricter Regulation.”* http://s.wsj.net/article/SB120631764481458291.html?mod=fpa_whatsnews

^{viii} “Principles-based regulation is essentially about outcomes or ends while rules-based regulation is about means. Principles-based regulation allows firms to decide how best to achieve required outcomes and, as such, it allows a much greater alignment of regulation with good business practice A more principles-based approach allows [organizations] increased scope to choose how they go about this. In short, the use of principles is a more grown-up approach to regulation than one that relies on rules.” Source: John Tiner, “Principles based regulation: the EU context” (http://www.fsa.gov.uk/pages/Library/Communication/Speeches/2006/1013_jt.shtml). “Our rules-based regulatory system is prescriptive and leads to greater focus on compliance with specific rules. We should move toward a structure that gives regulators more flexibility to work with entities on compliance within the spirit of regulatory principles.” Source: Hank Paulson, US Treasury secretary, speech to the Economic Club of New York in November 2006.

^{ix} Deloitte’s “Disarming the Value Killers” research identified that nearly 50% of \$1B+ companies lost

20% or more of their share price in less than a month during the past 10 years - some never recovered. Eighty-percent of these losses were the result of the interaction of multiple risk factors with most major losses resulting from a series of high-impact but low-likelihood events. In most of these organizations, risk management was scattered across specialist silos that did not talk with each other.

http://www.deloitte.com/dtt/cda/doc/content/us_assur_Value%20Killers%20Report%20.pdf

× Steve Hunt, of Hunt Business Intelligence, sizes the physical security market at \$150 billion (a number he leverages from Lehman Brothers) and states that the IT security market is roughly one fifth of this at \$30 billion. Corporate Integrity estimates that its GRC market figures only represents 5% overlap with the physical and IT security market figures.