

**GRC Strategic Agenda:**  
**The Value Proposition of Governance, Risk, and Compliance**

February 2008

~ Underwritten, in Part, by ~

## Executive Summary

Governmental, industry-wide, and organizationally imposed compliance and security regulations have placed a tremendous amount of focus on one of the most important, yet intangible assets an organization possesses: its data.

Given the multitude of risks prevalent in today's market, this report guides organizations towards implementing Governance, Risk, and Compliance (GRC) initiatives in a top-down, proactive, and business-advancing manner. By examining and analyzing Aberdeen data compiled from over 800 global organizations surrounding three of the most important and financially relevant aspects of a GRC initiative: compliance regulations, data security, and risk management, Aberdeen highlights and offers guidance on organizational focus and resources that contribute to bottom-line success.

Due to the tech-intensive nature of GRC solutions, it is often difficult to communicate their importance and value to upper-level decision makers. Geared towards C-suite budget holders, this report emphasizes the overall *business advantages* (rather than just IT) of a comprehensive GRC initiative.

Many organizations view a GRC initiative as a reactive and isolated quick-fix to achieve compliance, manage risk, or protect data. Highlighting the top-level business benefits, this report offers clear and actionable analysis about the importance of proactively managing risks and provides a roadmap showcasing the advantages and opportunities that exist when GRC initiatives are seen for what they are: holistic, enterprise-wide initiatives that become part of the organizations' DNA.

### Report Overview

---

- **Chapter 1.** Why governance, risk management, and compliance solutions are needed, the challenges organizations face with implementation, and the types of solutions that organizations deem most important.
- **Chapter 2.** How organizations view regulatory mandates, their intrinsic connection to risk management and data security, and the business case for adopting solutions regarding compliance. Providing a drill down example of the drivers, strategic actions, processes, solutions, and organizational attributes critical to a successful GRC initiative - data security.
- **Chapter 3.** The high-level importance risk management plays in GRC initiatives and the interconnectivity between managing risks and implementing GRC solutions in the increasingly regulated and competitive marketplace.
- **Chapter 4.** Weaving together the components of GRC to outline a roadmap that provides organizations with the ability to evaluate the current status of their GRC initiative and provide direction on the path that initiative can take to augment and proactively advance

[Send to a Friend](#) 

## Table of Contents

Executive Summary.....	2
Report Overview .....	2
Chapter One: The Need For and Challenges Surrounding GRC.....	4
Driving the Need for GRC.....	4
Implementing a Successful GRC Initiative .....	5
Chapter Two: Regulatory Compliance.....	7
Regulatory Compliance - Driving Implementation.....	7
No Policy - Little Governance .....	7
Do it Now - Do it Right.....	8
Security Trends.....	10
Chapter Three: Risk Management.....	14
Defining the Importance of Risk Management.....	14
Staying Ahead of Risk.....	15
Siloed Processes and Applications - The Big Risk in Your Own Backyard .....	16
Chapter Four: Solution Selection Strategies .....	20
Appendix A: Research Methodology.....	23
Appendix B: Related Aberdeen Research.....	24

## Figures

Figure 1: Key Pressures Driving Investment in GRC Solutions .....	4
Figure 2: Anticipated Problems in Implementing GRC Solutions.....	5
Figure 3: What Organizations Need in a GRC Solution.....	6
Figure 4: Top Factors Driving Focus on Security and Risk Management Initiatives.....	7
Figure 5: Maturity of Governance and Risk Management Programs.....	8
Figure 6: Organizational Attributes Designed to Improve Security and Risk Management.....	9
Figure 7: Most Important Standards / Regulations Driving Investment in GRC (1 = Low, 5 = High) .....	12
Figure 8: Organizational Trends Highlighting the Business Value of GRC Solutions .....	13
Figure 9: Top Factors Driving Organizations to Focus Resources on Loss Prevention.....	14
Figure 10: Top Strategic Actions for Managing Risk and Preventing Information Loss.....	16
Figure 11: Current Performance in Sensitive Data Protection .....	17
Figure 12: Impact of GRC Solutions on Optimizing Existing Business Processes.....	19

## Chapter One: The Need For and Challenges Surrounding GRC

### Driving the Need for GRC

The rise of government-mandated compliance regulations, coupled with the increasing need to safeguard sensitive data is forcing organizations to reconsider how their data is stored, accessed, secured, and managed. Inherently linked to this challenge is the need to objectively assess and proactively manage the growing number of risks prevalent in the market.

In addition to these pressures, the escalation of a global competitive marketplace resulting in frequent mergers, acquisitions, and re-structuring demand that organizations focus resources to improve both the quality and control mechanisms surrounding their data.

Aberdeen Group research from [The Information Governance Benchmark Report](#), reveals that the top business pressures driving organizational investment in GRC software and solutions is the need to comply with external and internal regulations (Figure 1).

**Figure 1: Key Pressures Driving Investment in GRC Solutions**



At a basic level there are two broad reasons organizations are implementing GRC programs:

- Outside regulatory bodies are telling them to; or
- They are aware of the potentially enormous monetary and / or reputation risks of *not* having such a program in place.

A critical first step to understanding which GRC initiatives are best suited to an individual organization involves comprehending the macroeconomic pressures that drive the adoption of GRC initiatives.

#### Fast Facts

√ X% type statistic description here

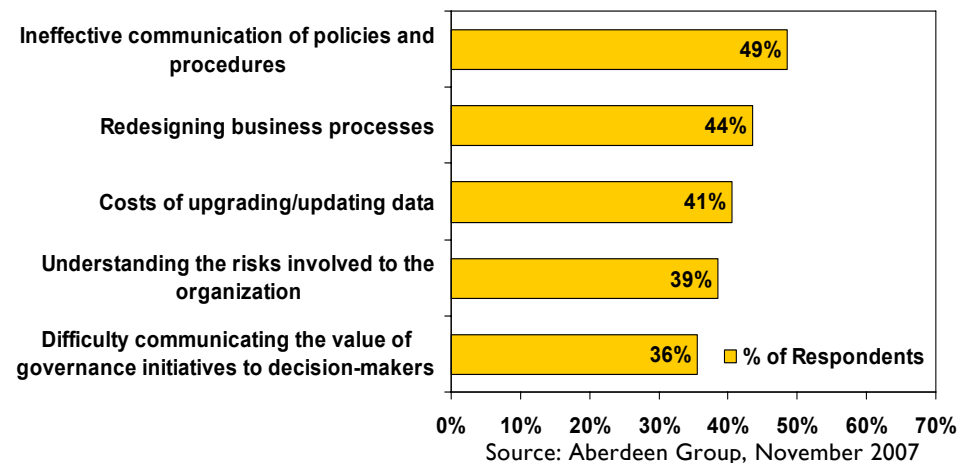
√ X% type statistic description here

### Implementing a Successful GRC Initiative

Public outcry associated with large-scale fraudulent accounting principles has resulted in dramatically heightened regulatory requirements. Ineffective security and risk management programs have detrimentally affected organizations to the tune of millions, and sometimes billions of dollars. These widely publicized issues, coupled with the converging and increasingly fluid dynamic of the technology market has brought the term GRC to the boardroom. The challenge is to comply with new sets of oft-confusing regulations while keeping data secure and increasing operational efficiency to meet growing competitive pressures.

There are numerous benefits of a comprehensive GRC initiative. However, getting to that proverbial promised land is neither simple nor cheap. Even with a carefully crafted and detailed pre-implementation plan, and especially without one, organizations can encounter a variety of challenges associated with implementing their GRC initiatives.

**Figure 2: Anticipated Problems in Implementing GRC Solutions**



Problems associated with the ineffective communication of policies and procedures are most often rooted in the organizational structure. In particular, the presence of organizational silos in large-scale regional or multi-national companies is a major hurdle.

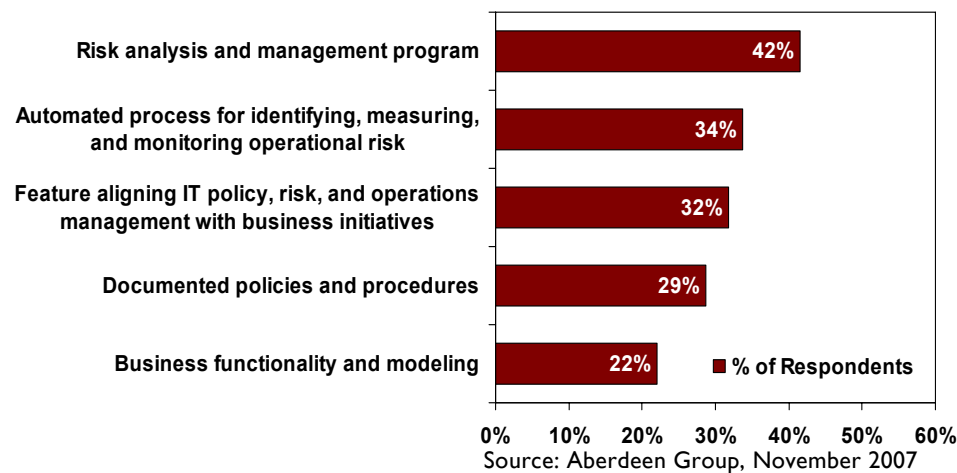
This problem is especially painful when trying to identify and manage risk. Often, these silos don't communicate with each other which can significantly cloud the enterprise-spanning visibility needed for effective risk management. To combat this problem, a number of organizations have adopted risk convergence policies and procedures. Having the potential risks from each disparate organizational division funnel into a centralized repository allows risks to be identified, evaluated, prioritized, and managed based on a complete and enterprise-encompassing risk picture. Also, it has the added advantage of avoiding time consuming, costly, and unnecessary redundancy issues. Organizations should not have to spend time and money

alleviating problems and risks that have already been overcome and managed.

Mapping a uniquely tailored GRC initiative to strategic goals should be a primary objective of organizations considering either an initial investment or when seeking to re-vamp an unsuccessful implementation.

The importance an organization places on the various features provided by a GRC solution can vary, sometimes significantly, given the individual goals of that organization. However, there are some features, such as automated processes for risk analysis and management, and the ability to align IT policy, risk and operations management with business initiatives, that organizations identified as most important when deciding whether to invest in a GRC solution (Figure 3).

**Figure 3: What Organizations Need in a GRC Solution**



### Aberdeen Insights - Desired Vendor Traits

Provided a solution set matches up with an organization's needs, the next step an organization needs to consider are the traits the vendor company as a whole embraces and projects into the market. Aberdeen research reveals that organizations seeking to invest in data governance solutions found the following to be the most important characteristics of a potential solution provider:

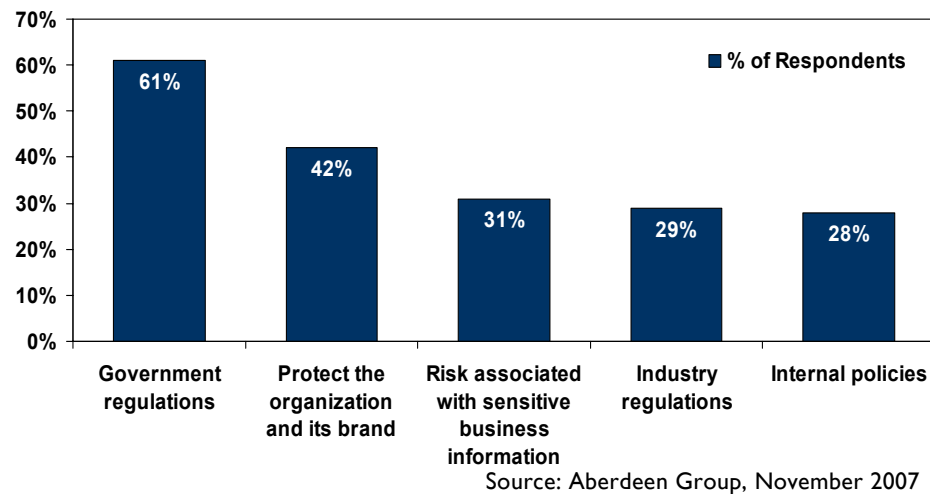
- Vision and strategy (39%)
- Integration with legacy systems and related technologies (35%)
- Professional services breadth and depth (30%)
- Financially sound (25%)
- Market leading products (23%)

## Chapter Two: Regulatory Compliance

### Regulatory Compliance - Driving Implementation

Security and compliance play a vital role in the structuring of a data governance initiative in general, and provide the foundation on which a GRC initiative is built, in particular. Hence, it should come as no surprise that the top factor driving organizations to focus resources on security and risk management initiatives is the need to comply with governmental regulations (Figure 4).

**Figure 4: Top Factors Driving Focus on Security and Risk Management Initiatives**



Both government and, to a lesser extent, industry regulations are critical external drivers. There are, of course, internal drivers. The most important of these is protecting the organization and its brand. The potential impact on brand and, ultimately, corporate reputation offers a crystal-clear view of the importance of establishing and maintaining organizational data that is both secure and compliant. Employees in every function and at all levels can attest to the catastrophic long-term impact on revenue and profitability of a single instance, let alone frequent public disclosures, of security breaches involving personal information / data about their own customers.

### No Policy - Little Governance

The G in GRC is often the most difficult. Currently, the top strategic action taken by organizations to drive investment in governance and risk management is the establishment and enforcement of consistent policies and procedures. Important in transitioning this action to fulfillment is taking ownership of risk assessment and fully documenting the processes, risks,

and controls and continually mapping them back to ensure they fully align with the business goals.

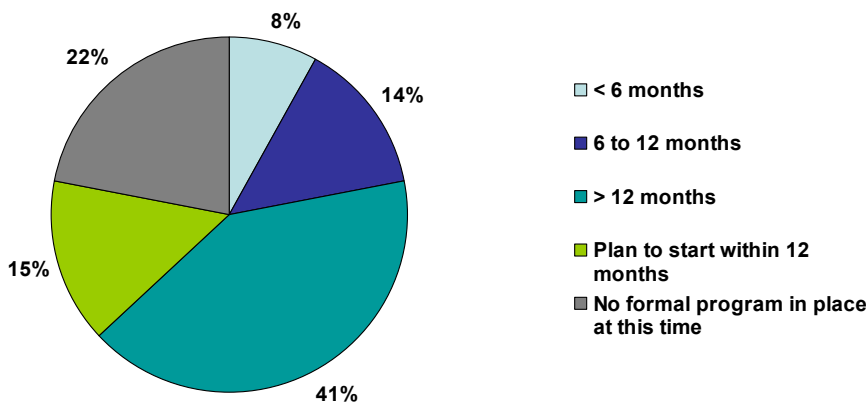
From a technology perspective, this strategic action can be supported by the development of a sustainable, "continuous" compliance infrastructure created via the astute application of automation, process streamlining, and simplification.

Built upon specific and unique levels of risk tolerance, these actions create a foundation and stepping-stone allowing organizations to advance as they continue the pursuit of business improvement. For example, an organization competing in a heavily regulated industry such as banking or finance, with a very low risk threshold requires a sustainable, continuous compliance infrastructure wholly supported by enterprise-wide documented policies, processes, and procedures. While this may sound obvious, the absence of either one of these elements leads to disaster.

### **Do it Now - Do it Right**

Aberdeen research reports that only 41% of organizations have a mature governance and risk management program (in place over 12 months). In contrast, 22% reported having no formal program in place (Figure 5). Without a formal program, these organizations will be compelled to respond to new and existing requirements on an ad hoc basis.

**Figure 5: Maturity of Governance and Risk Management Programs**



Source: Aberdeen Group, November 2007

Such a fragmented approach leads to a patchwork of disparate policies and processes that result in an inconsistent approach to governance and renders it virtually impossible to proactively assess and accurately manage risks. This will increase vulnerability and tend to encourage sub-optimal implementations of security efforts on a departmental or regional basis. Ultimately, without a holistic and integrated GRC framework, there will be limited cohesion and little success when implementing the enterprise-wide changes necessary to address mandated industry, governmental, and corporate regulations and adequately manage growing operational risks.

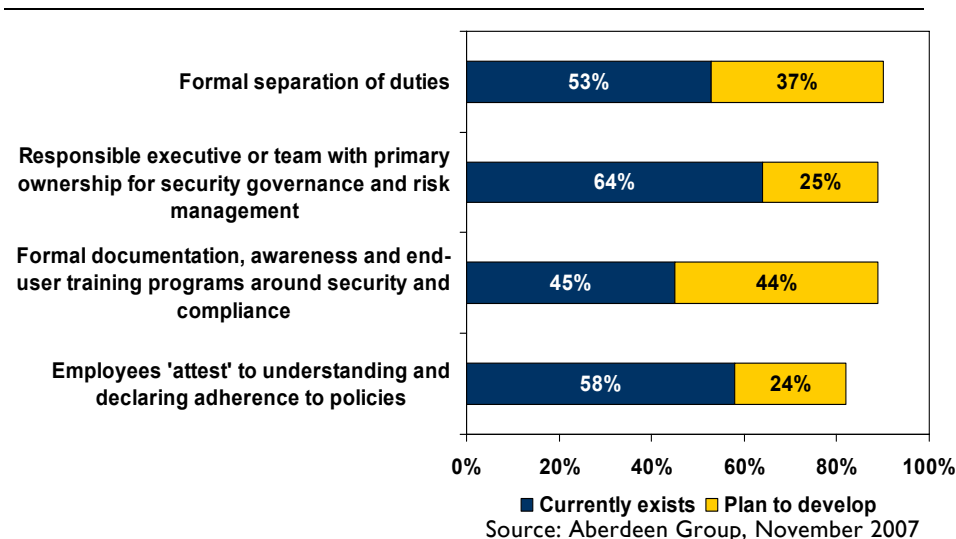
As would be expected, there exists a distinct correlation between the length of time and amount of money that an organization has invested in its GRC program, and the effectiveness of their plans and capabilities.

*Organizational Attributes and Capabilities Improving Security and Compliance*

One of the most common and widely discussed areas of GRC involves the intersecting areas of IT security and risk management. Focusing on this important aspect of GRC offers the opportunity to both drill down and reveal capabilities and strategies that are equally applicable to governance and compliance, as well as sharpening the picture on the importance and business value of GRC initiatives as a whole.

As Figure 6 indicates, one of the most important attributes an organization can possess is to have a responsible executive or team with primary ownership for security governance and risk management.

**Figure 6: Organizational Attributes Designed to Improve Security and Risk Management**



Having a dedicated executive or cross-functional team taking ownership of the GRC initiative is important for a variety of reasons. One reason is that it addresses the disconnect that often exists between the IT and business factions within an organizational structure.

Understanding and aligning both the IT issues and business goals that influence and determine the scope of a governance program is critical to ensuring its success and longevity. Highlighting this need for alignment, Aberdeen research has reported that almost 91% of organizations either have or are currently developing capabilities that allow management to be accurately informed of IT-dependent risks.

A good example of how tech-intensive GRC tools can be leveraged to show value to the C-Suite involves automated risk and compliance related report generation. The daily GRC process owners and IT staff can have access to drill-down reports that provides them the highly technical minutia necessary to proactively ensure compliance or mitigate risk. The message of these reports would ordinarily be lost on upper management whose focus is fixed on high-level business issues. Although currently being used in only 22% of surveyed organizations, a GRC solution with the capability to deliver the technical drill down reports, while also generating executive dashboards (essentially tracking high-level changes from the previous report and/or highlighting top-level decreases in risk and increases in compliance) constantly validates the business value of GRC solutions to the C-Suite.

Additionally, 89% of organizations either already have or plan to develop formal documentation, awareness, and end user training programs around security and compliance. Although important by itself, when combined with a requirement that employees "attest" to understanding and adhering to GRC policies, these awareness and training programs result in a company-wide mindset where employees not only understand the importance of data security and compliance, but also proactively involve themselves with achieving GRC goals.

In addition to developing and fostering an organizational culture that works to advance security and compliance, organizations are using a variety of technologies targeted specifically at security as a part of their overall GRC program.

Central to securing data is managing and monitoring access to organizational networks. 78% of organizations either implement or plan to implement some type of network access control. Similar percentages exist for implementing management over databases and logs. Additionally, over 75% of companies have capabilities in place that help manage and monitor change. Understanding how systems and applications have changed, and are being changed, creates the visibility needed to apply strong security governance policies.

However, the numerous benefits associated with implementing the technologies discussed earlier cannot be fully realized unless the overall GRC initiative is first viewed through an enterprise-wide lens. For example, only 46% of surveyed organizations currently have controls to monitor and verify that requirements of internal policies and external regulations are being satisfied. Additionally, only 26% currently have automated testing of these controls. Documentation, as discussed earlier, is vital in this regard.

## **Security Trends**

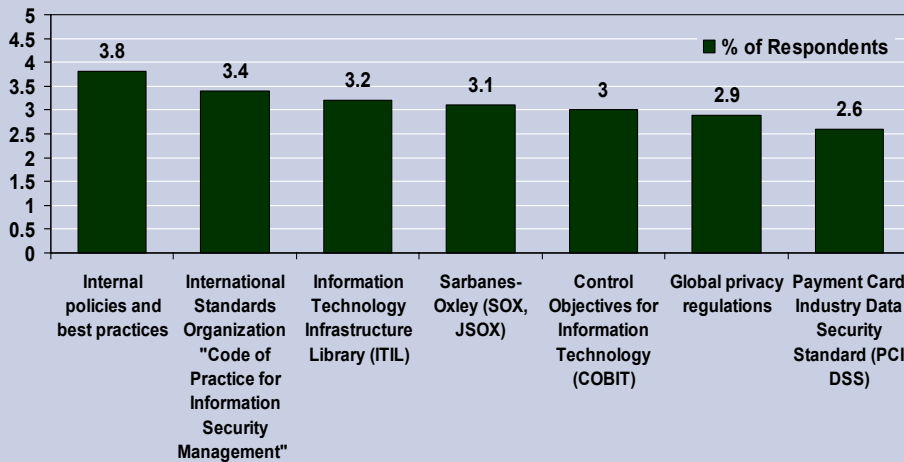
As the number and variety regulations continues to rise, it comes as no surprise that 64% of organizations responded that the percentage of their sensitive information needing protection increased over the past 12 months. As such, organizations are dedicating more resources for GRC initiatives which directly impact the level of prioritization given to such programs.

Another trend that reveals a significant opportunity in the GRC space is the increasing number of organizational and geographical "silos" being created for security governance, risk management, and compliance information and analysis. Solutions that standardize and automate controls across these silos will help decrease the time required to mitigate security, compliance, and risk related incidents.

**Aberdeen Insights - Compliance Trends**

Compliance is the factor that most significantly impacts the acceleration and adoption of data governance initiatives. There are myriad regulations to which organizations must comply. Figure 7 displays a selection of those that organizations have identified as most important.

**Figure 7: Most Important Standards / Regulations Driving Investment in GRC (1 = Low, 5 = High)**



Source: Aberdeen Group, November 2007

Governmentally imposed regulations such as SOX and PCI DSS make the list of most important regulations. The intricate and detailed nuances of these regulations are legendary, and achieving compliance with all aspects of them requires a detailed and through approach.

Also significant is the lack of any one regulation achieving a very high level of importance. The importance of each of these key regulations distribute closely about the midpoint of the rating scale. This implies a growing fatigue with regulations that may have organizations responding to them as more of a common event than as something necessitating a unique response.

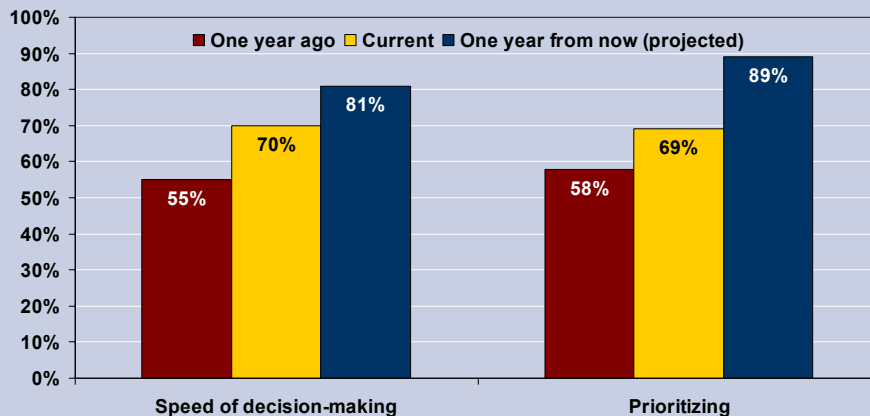
Important to note is the fact that internal policies and best practices emerged as the most important regulation(s). Internal policies, if holistically derived and clearly articulated, can offer the greatest rewards. Also, policies backed by on-site executives often get more attention than those backed by some amorphous agency - no matter what the consequence. Additionally, this indicates that there has been a shift from compulsory regulations such as SOX being the primary driver of GRC implementations, to organizations implementing GRC programs because it makes good business sense.

### A View From the Top: Security and Compliance - Why it Matters to the CFO

Process owners in organizations of all sizes implicitly understand the variety of benefits that a comprehensive, effectively implemented GRC solution can provide. However, the highly technical nature of the solutions often makes it difficult to convey the high-level business value benefits sufficiently for the Chief Financial Officer (CFO) and other executives to approve the project and allocate the requisite budget. In fact, one of the key problems organizations indicated they anticipate encountering when implementing a GRC solution is difficulty communicating the value of such solutions to decision makers (36%).

In communicating the value of GRC solutions to the C-suite budget holders, metrics that highlight the business value of GRC solutions are invaluable. In business, time is money. Showcasing the impact GRC solutions have on an organization's ability to prioritize investments based on defined business objectives and on speed of decision making represent ways process owners can arm themselves with top-line examples that make the business case for adopting these solutions (Figure 8).

**Figure 8: Organizational Trends Highlighting the Business Value of GRC Solutions**



Source: Aberdeen Group, November 2007

The next chapter discusses the vital, interconnected role risk management plays in GRC initiatives.

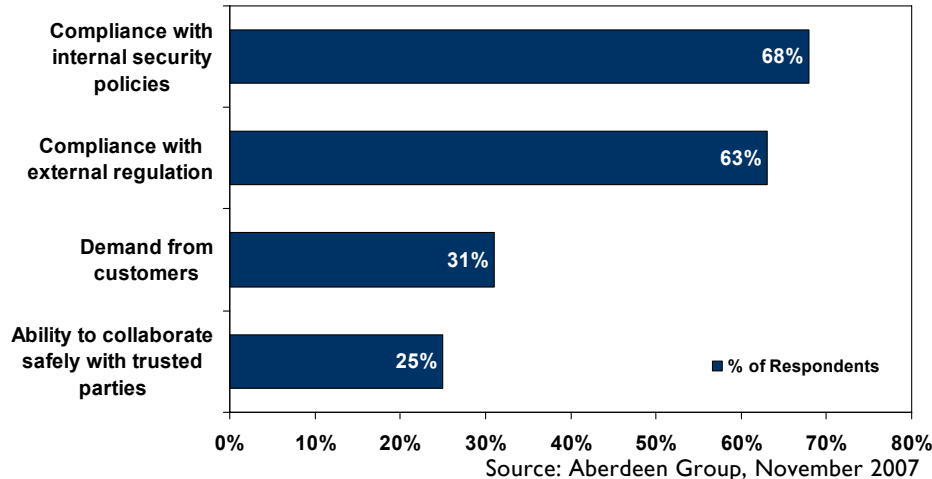
## Chapter Three: Risk Management

### Defining the Importance of Risk Management

As Figure 3 in Chapter One highlighted, the feature organizations desire most in a GRC initiative is the capability to analyze and manage risk (42%). As the complexity and volume of governmental, industry, and internal regulations continue to rise, risk management programs that involve cumbersome and error-prone manual processes are being viewed by end users as outdated and ineffective. In fact, organizations view the ability to provide an automated process for identifying, measuring, and monitoring risk (34%) as the second most important feature a GRC solution can offer.

At its core, risk management deals with mitigating or avoiding a loss event. Further showing the interconnectivity between governance, risk, and compliance, Aberdeen research found that the top two factors driving organizations to focus resources on data protection / loss prevention deal with compliance issues (Figure 9).

**Figure 9: Top Factors Driving Organizations to Focus Resources on Loss Prevention**



A critical first step for GRC initiatives in general, and risk management in particular, is to understand what the organizations loss events are. Equipped with this knowledge, an organization can then determine the necessary processes to put in place to make sure it doesn't happen again.

Compliance concerns are forcing organizations to both re-think the priority risk management solutions receive, and re-invest in GRC solutions that offer comprehensive risk management coverage. From an enterprise perspective, organizations value GRC solutions that are equipped with automated controls that proactively identify and manage the risks associated with failing to comply with external regulations. This is particularly important to the

large number of organizations that provide services or products in multiple markets because they are required to comply with a variety of complex governmental and industry-specific regulations.

### **Aberdeen Insights - Extending Risk Management Beyond Financial Services**

For many organizations, particularly those competing in heavily regulated industries subject to a variety of regulations such as banking, financial services, energy and utilities, and pharmaceutical manufacturing, a large part of a GRC initiative involves strategies around minimizing a loss event through focusing on oversight, assurance, and risk management. Effective GRC initiatives take into account and manage both enterprise and operational risks. The thin line between risk and reward can be most efficiently traversed once an organization assesses the enterprise-spanning risks alongside future goals. Mapping and managing these two critical assets and opposing pressures together provides an organizational framework built to minimize risk and achieve strategic objectives.

Due to its highly prevalent and widely publicized use in financial service organizations, holistic and integrated risk management processes in general, and Enterprise Risk Management (ERM) in particular, are sometimes viewed by organizations outside financial services as unnecessary.

Years ago government mandates (such as the introduction of mandatory and strictly enforced SOX compliance regulations) provided the "oh no" moment when financial service organizations fully grasped the need for GRC initiatives. That moment is quite possibly looming for a variety of organizations outside the financial services sector with Standard and Poor's (S&P) proposal to introduce ERM analysis into the corporate credit ratings process globally.

If the proposal passes, S&P analysts and rating committees would include ERM capabilities and processes when evaluating non-financial company's credit ratings. Companies would have to answer a variety of detailed questions regarding each of the four major sub-categories of ERM that S&P has outlined including: 1.) risk management culture and governance, 2.) risk controls, 3.) emerging risks, and 4.) strategic risk management.

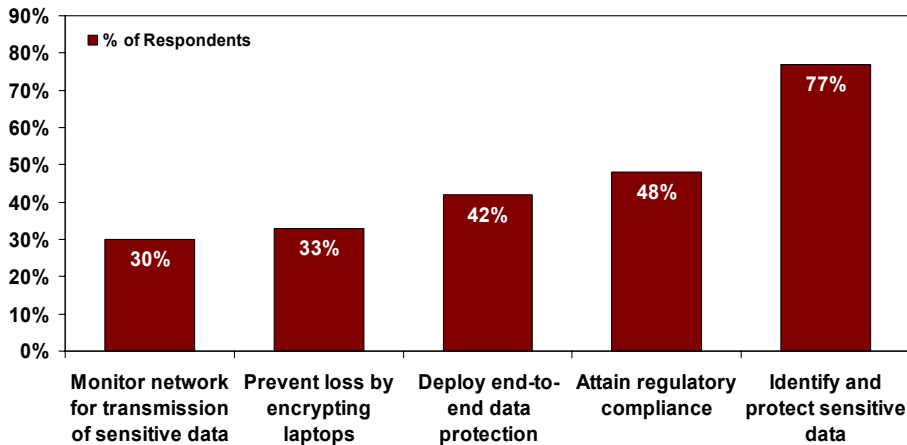
Although the comment period on this proposal has been extended to March 1, 2008, this should serve as a wake-up call to the hundreds of non-financial organizations that could potentially be detrimentally affected.

### **Staying Ahead of Risk**

Risk management is based on the premise that, through implementing the correct GRC solution, organizations can analyze, identify, and thus manage risk proactively. At a very basic level, risk management ensures potential risks are dealt with before they develop into high-dollar problems. To accomplish this, the top strategic action organizations are taking to manage

risk and prevent a loss event is to identify and protect sensitive data. (Figure 10)

**Figure 10: Top Strategic Actions for Managing Risk and Preventing Information Loss**



Source: Aberdeen Group, November 2007

From an enterprise perspective, protecting sensitive data is a necessity. However, as the sheer volume of sensitive data rises, organizations without an effective GRC solution are finding it difficult to ensure that data is protected. In fact, less than half of organizations (48%) responded that the percentage of sensitive data that is adequately protected from outsider attack has improved over the past two years. Over the last year alone, there have been countless heavily-publicized and extremely costly examples of the dangers of not protecting sensitive customer data. Without comprehensive risk management processes in place that allows an organization to not only understand their potential losses but also how to mitigate them, the organizations remains continuously vulnerable to a costly and embarrassing unforeseen loss event.

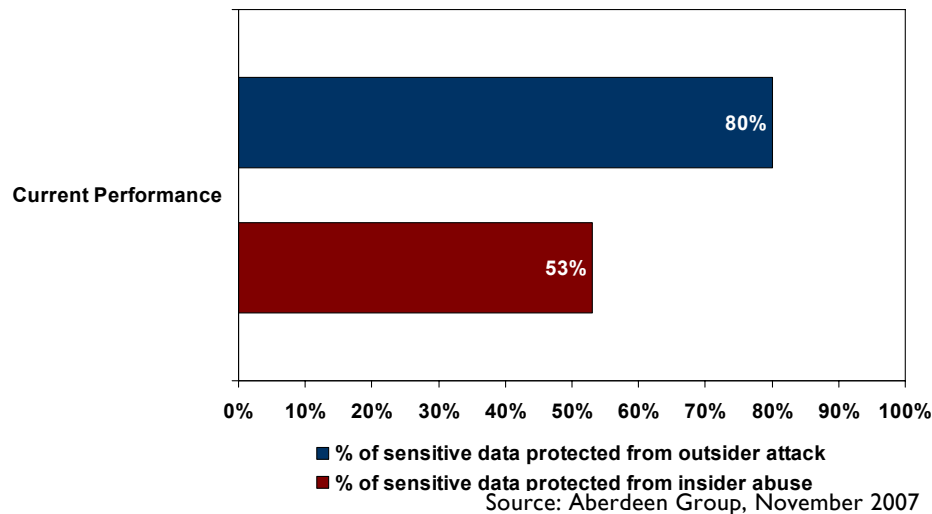
### ***Siloed Processes and Applications - The Big Risk in Your Own Backyard***

When evaluating a GRC solution, many organizations find it beneficial to narrow their focus and determine how that solution will impact their local applications and devices. With the steadily increasing rise of mobile and remote workers, it comes as no surprise that one of the top actions organizations are taking to manage risk and prevent information loss is to ensure that laptops are properly protected (33%).

Certain workers, both in and away from the corporate office, will continue to have the need to access sensitive data; thus encrypting laptops to protect that data from outsider attack is undoubtedly important. However, a comprehensive risk management and GRC solution ensures that only the right workers have access to sensitive data to begin with.

As evidenced by news stories around the globe, insider abuse of sensitive information is a reoccurring, embarrassing, and extremely costly problem. Despite the heavily-publicized nature of these types of problems, less than half (47%) of surveyed organizations reported an improvement in the percentage of sensitive data that is protected from insider abuse over the preceding two years. Even more alarming is the fact that, on average, organizations responded that currently only 53% of their sensitive data is adequately protected from insider abuse (Figure 11).

**Figure 11: Current Performance in Sensitive Data Protection**



Compounding the problem, data from Aberdeen Group's July 2007 benchmark study, [Delivering Actionable Information to the Enterprise: Does On-Demand BI Solve the Skill Set Shortage?](#) shows that 72% of organizations use Microsoft Excel as the primary vehicle to formulate and share data across the organization. The highly prevalent use of spreadsheets and the relative ease with which they can be accessed, shared, and even changed represents a large risk for organizations of all sizes. A solution that offers the ability to control who and how data-sensitive spreadsheets will be accessed proactively mitigates a large portion of the risk associated with insider abuse.

### *Ignorance Is Not Bliss*

Many organizations, particularly those that are large, multi-national, or competing in a multi-regulatory environment are not even aware of the potential risks. As the number of organizational and geographical "silos" for governance, risk management, and compliance information and analysis grows (only 15% of organizations responded that the number of these silos decreased over the past 12 months), it is virtually impossible for in-house staff to properly manage risk with a homegrown solution or on a disjointed basis.

Another major disadvantage of operating in silos is that oftentimes, there is no common language; the same risk can be phrased differently resulting in redundant and costly unnecessary mitigation. Without convergence and integration of risk processes and controls, there is no common framework to identify, prioritize, and communicate these risks through the necessary channels. Further compounding the problem, some of the silo operators don't want it to change. This is yet another example of the importance of a top-down, organizational-wide approach to GRC implementation.

Also, organizational silos frequently employ manual risk management processes that are cumbersome, costly, and extremely time-intensive. In addition, these processes are frequently skewed by the subjective views that a risk assessor / analyst will have about the nature and likelihood of a given risk. The result is that risks are often mis-prioritized. Time and money are unintentionally misdirected towards risks that are minor, while major risks (mischaracterized by manual processes as minor) are not properly mitigated or monitored. A GRC solution with the ability to integrate into a legacy or homegrown system and objectively automate risk analysis, identification, prioritization, and management is a critical component of a comprehensive GRC solution.

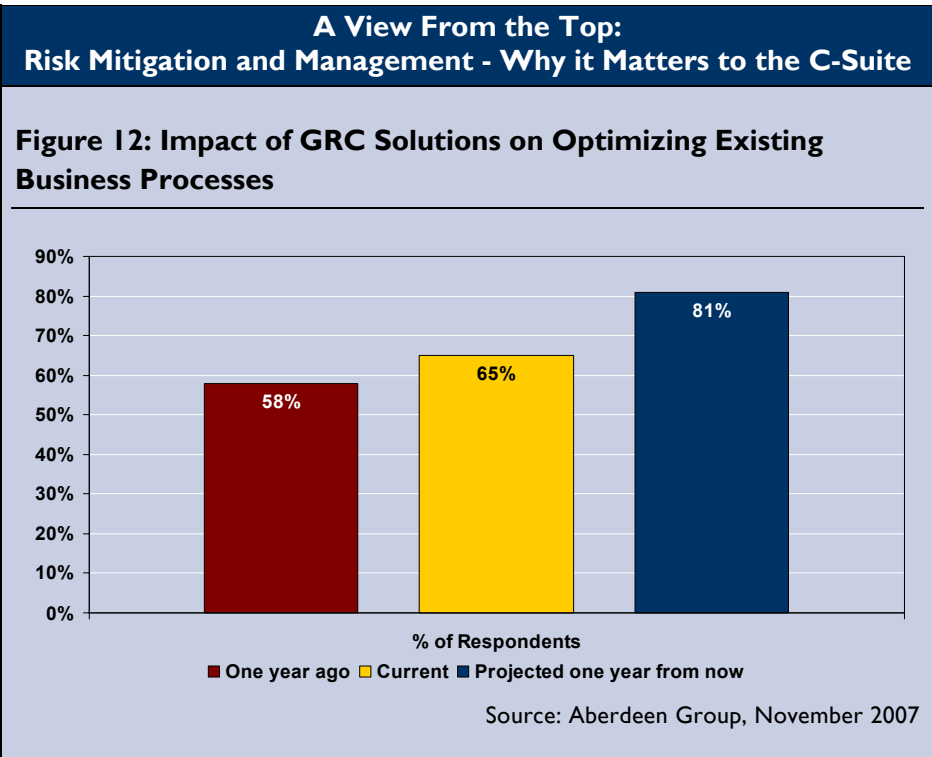
#### **A View From the Top: Risk Mitigation and Management - Why it Matters to the C-suite**

Because the goal of risk management is to stop a potentially costly problem before it occurs, it is often difficult to communicate the bottom-line value of implementing a GRC solution to upper-management. Similar to proving a negative, showing a definitive Return on Investment (ROI) from a loss event that didn't occur is often difficult to accomplish.

An effective way to end-run this problem is to provide the CFO with concrete examples that highlight the bottom-line business value of incorporating a comprehensive GRC solution into the organizational framework. When justifying a potential investment in a GRC solution to upper-management, complex technological "deep-dives" into the individual components of the solution can muddy the waters; leading off with the overall business benefits is one of the fastest ways to engage C-level executives and an important stride on the road to receiving their stamp of approval.

For example, 34% of organizations indicated that their current risk management and information loss solutions decreased user productivity. Speaking directly to how this negatively impacts the business, and showcasing how implementing a holistic and efficient GRC solution can directly address these issues by, among other things, optimizing existing business processes helps show how such solutions alleviate the pressures and pains that are top of mind to the C-suite (Figure 12).

*continued*



### Case Study - XXX

[This section is currently blank.]

## Chapter Four: Solution Selection Strategies

The increasing barrage of governmental, industry specific, and internal regulations, coupled with the pressures of increased competition and risk in a global market has clearly defined the need for organizations of all sizes to implement GRC initiatives. However, quick-fix solutions put in place on a reactive basis targeted towards alleviating a problem that has already occurred is a costly and ineffective method.

Continuing this reports high-level message without detailing the merits of the countless solution types offered beneath the spanning GRC umbrella, and emphasizing the business value of a proactive, integrated, and top-down driven enterprise-wide GRC implementation, the following sections represent a basic roadmap that organizations can leverage to: 1.) initiate a GRC framework, or 2.) evaluate the current status of their GRC initiative and gain insight on the path that initiative can take to augment and proactively advance their business goals.

- **Thoroughly evaluate the forward-thinking business goals your organization is focusing on.** The establishment of a cross-functional team comprised of high level business executives, line of business managers, future process owners, and IT executives and staff is invaluable to ensure the potential owners and daily operators of the GRC initiative are on the same page in terms of the overall business goals that need to be advanced.
- **Develop a clear picture of the current problems facing your organization and potential stumbling blocks in the future.** This is a critical step to avoid costly and repetitive quick-fix solution deployments. To understand how a GRC initiative can alleviate current and future problems while advancing business goals, the organizations must first have a deep understanding of what those problems are.

Although a truly effective enterprise-wide GRC initiative becomes part of the entire organizational structure itself, prioritizing current and future problems by timing and scope allows organizations to direct the proper focus on immediate risks.

- **Evaluate the current state of your organizations internal capabilities and structure.** The “G” in GRC is often the most difficult. By evaluating your organizations current capabilities and structure, you can develop an organizational framework that can fully support your GRC initiative.

Education and training are particularly helpful here. Knowing employees will be responsible for the various aspects of the initiative, and properly training them on the required processes, controls, and information flows will save a tremendous amount of time, money, and headaches.

### Fast Facts

√ **X%** type statistic description here

√ **X%** type statistic description here

A good governance framework incorporates training, continual monitoring, sufficient processes and controls, and clearly delineated roles and responsibilities. A great governance framework incorporates everything already mentioned, but is built on a foundation of company-wide knowledge, understanding, and belief that each employee has a stake in advancing the goals of the business.

- **Evaluate potential providers on their ability to alleviate current problems.** Although the message of this report emphasizes a holistic and proactive approach to GRC initiatives some organizations, mainly for regulatory compliance or risk management concerns, have an immediate need for a GRC solution. If your organization falls into this category, reviewing the first two recommendations will ensure that your solution not only addresses a problem you really need to have solved, but also ensures that its implementation will advance your business goals.
- **Map the capabilities of the potential provider back to the business goals your organization will be focusing on in the future.** Scalability is critical here. Ensuring the potential provider has the capabilities to scale their solution to your future needs and goals will allow you to proceed with confidence.
- **Determine whether the potential provider offers integration and / or convergence as part of their solution.** Especially important to large organizations, integration and convergence are critical to realizing business, not just IT, advances.

In terms of compliance, without integration, costly and time-consuming rules and processes can be set up for each organizational silo. Integrating all the organizations compliance requirements, rules, and processes simplifies and streamlines compliance reporting allowing the organization to realize cost savings that can be applied towards business goals as well as adjust much faster to new or heightened regulations.

In terms of risk management, risk convergence (both operational and business-oriented) provides a number of benefits. Viewing the entire spectrum of risks together allows the organization to effectively and objectively assess, prioritize, evaluate, and manage those risks in a comprehensive and cost-effective manner. This also ensures that the organization is focusing on the risks they should be, instead of wasting time and money focusing on a low priority risk, while leaving them vulnerable to a mis-prioritized risk that could severely damage reputation and revenue.

### **Aberdeen Insights - Summary: Why GRC Matter to the C-Suite**

The benefits associated with a comprehensive GRC initiative, such as better and more effective risk management, achieving compliance, as well as enhanced IT and organizational governance have been well documented.

However, the real benefit of an enterprise-wide, proactive, top-down driven initiative is the competitive advantage it offers in terms of top-line business value. The C-suite should be informed of the vast difference between a costly, inefficient, fragmented, reactionary, and piecemeal method to GRC implementation and the tangible business benefits derived from an informed, proactive, enterprise-wide approach.

Any CEO or CFO would agree that incorporating a comprehensive GRC solution before a costly problem develops, that manages risks and ensures compliance while advancing, rather than hindering business goals, is preferable to incurring potentially huge losses through non-compliant related fines or sensitive data leaks. Additionally, upper-level decision makers should realize that a proactive top-down approach ensuring that the initiative works in concert with and advances important business goals is preferable to a regulatory body mandating remedial actions and steps that must be taken without regard to their effect on company revenue or image.

*Send to a Friend* 

## Appendix A: Research Methodology

Over the past 12 months Aberdeen examined the use, the experiences, and the intentions of more than 800 global enterprises using Governance, Risk, and/or Compliance solutions in a diverse set of enterprises.

Aberdeen supplemented this online survey effort with interviews with select survey respondents, gathering additional information on GRC strategies, experiences, and results.

Responding enterprises included the following:

- *Job title / function:* The research sample included respondents with the following job titles: procurement, supply chain, or logistics manager; operations manager; IT manager or staff; sales and marketing staff; and senior management.
- *Industry:* The research sample included respondents from a variety of industries including: financial services, telecom, pharmaceutical, government, healthcare, retail, and manufacturing.
- *Geography:* The majority of respondents (52%) were from North America. Remaining respondents were from the Asia-Pacific region (26%) and EMEA (22%).
- *Company size:* Thirty-five percent (35%) of respondents were from large enterprises (annual revenues above US \$1 billion); 35% were from midsize enterprises (annual revenues between \$50 million and \$1 billion); and 30% of respondents were from small businesses (annual revenues of \$50 million or less).
- *Headcount:* Thirty percent (30%) of respondents were from small enterprises (headcount between 1 and 99 employees); 30% were from midsize enterprises (headcount between 100 and 999 employees); and 40% of respondents were from small businesses (headcount greater than 1,000 employees).

Solution providers recognized as sponsors were solicited after the fact and had no substantive influence on the direction of this report. Their sponsorship has made it possible for Aberdeen Group to make these findings available to readers at no charge.

### Study Focus

Responding executives completed an online survey that included questions designed to determine the following:

- √ The degree to which GRC solutions are deployed in their operations and the financial implications of the technology
- √ The structure and effectiveness of existing GRC implementations
- √ Current and planned use of GRC to aid operational activities
- √ The benefits, if any, that have been derived from GRC initiatives

The study aimed to identify emerging best practices for GRC usage and to provide a framework by which readers could assess their own management capabilities.

## Appendix B: Related Aberdeen Research

Related Aberdeen research that forms a companion or reference to this report include:

- [\*The Information Governance Benchmark Report\*](#); July 2006
- [\*Security Governance and Risk Management\*](#); November 2007
- [\*Master Data Management in Data Migration\*](#); April 2007
- [\*Customer Information Management: Data Quality and Integration\*](#); June 2006
- [\*Delivering Actionable Information to the Enterprise: Does On-Demand BI Solve the Skill Set Shortage?\*](#); July 2007

Information on these and any other Aberdeen publications can be found at [www.Aberdeen.com](http://www.Aberdeen.com).

Author: Stephen Walker, Technology Markets Group,  
[stephen.walker@aberdeen.com](mailto:stephen.walker@aberdeen.com)

Founded in 1988, Aberdeen Group is the technology- driven research destination of choice for the global business executive. Aberdeen Group has 400,000 research members in over 36 countries around the world that both participate in and direct the most comprehensive technology-driven value chain research in the market. Through its continued fact-based research, benchmarking, and actionable analysis, Aberdeen Group offers global business and technology executives a unique mix of actionable research, KPIs, tools, and services.

This document is the result of primary research performed by Aberdeen Group. Aberdeen Group's methodologies provides for objective fact based research and represent the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen Group, Inc. and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Aberdeen Group, Inc.

As a Harte-Hanks Company, Aberdeen plays a key role of putting content in context for the global direct and targeted marketing company. Aberdeen's analytical and independent view of the "customer optimization" process of Harte-Hanks (Information – Opportunity – Insight – Engagement – Interaction) extends the client value and accentuates the strategic role Harte-Hanks brings to the market. For additional information, visit Aberdeen <http://www.aberdeen.com> or call (617) 723-7890, or to learn more about Harte-Hanks, call (800) 456-9748 or go to <http://www.harte-hanks.com>

091707a