

July 20, 2009

## **What The Business Doesn't Understand About IT GRC**

Priorities And Perspectives From Business And  
IT Professionals

A commissioned study conducted by Forrester Consulting on behalf of  
EMC Consulting

FORRESTER®



**Headquarters**

Forrester Research, Inc., 400 Technology Square, Cambridge, MA 02139 USA  
Tel: +1 617.613.6000 • Fax: +1 617.613.5000 • [www.forrester.com](http://www.forrester.com)

## TABLE OF CONTENTS

Executive Summary .....	3
IT Risk And Compliance Programs Face Mounting Challenges .....	5
IT GRC Is Key To Meeting Business Needs .....	6
IT GRC Alignment Needs Some Adjustment .....	11
IT Requires More Perspective From The Business.....	11
Cost Continues To Be A Major Business Concern.....	13
IT Does Not Effectively Communicate Its Value .....	15
Recommended Steps Toward Improvement.....	19
Appendix A: Methodology .....	20

© 2009, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to [www.forrester.com](http://www.forrester.com).

## Executive Summary

In May 2009, EMC Consulting commissioned Forrester Consulting to evaluate the priorities, practices, and perceptions of IT governance, risk, and compliance (GRC). An increasingly common methodology among mature IT departments, IT GRC is the set of efforts aiming to coordinate key elements of risk and compliance programs (e.g., risk assessments, control assessments, remediation, reporting) to gain greater efficiency and improve oversight.

The rise of IT GRC programs corresponds to the difficulty companies face in their attempts to comply with increasingly demanding regulatory requirements and manage greater risks associated with more complex business and IT environments. While many IT GRC programs are showing significant value, however, there is often a substantial gap between the efforts undertaken within the IT department and the expectations that are understood by business professionals.

Various conditions are responsible for this gap. IT risk and compliance professionals have tended to be more security-minded, focusing on threat and vulnerability mitigation, correct patches and configurations, and automated controls. The enterprise risk and compliance perspective has tended to focus more on risk likelihood and impact, taking risk for reward, and achieving compliance through written policies and manual controls. IT GRC programs must primarily focus on the IT risks and controls for which they're responsible, but as they are asked to support enterprise GRC programs and the business at large, they will have to better understand what is expected of them and how to meet those expectations.

Forrester conducted in-depth surveys with 116 IT professionals responsible for risk and compliance, as well as 106 business professionals with responsibility for or influence over at least some aspects of IT risk and compliance. Forrester found that there were many similarities in how business and IT professionals viewed the value and efforts of their IT GRC programs. In addition, of the eight IT GRC projects we asked about that companies have taken on in the past year, each was rated by at least 50% of business respondents as having a positive impact on the business as a whole.

Despite some of the positive results perceived with IT GRC projects, business and IT professionals still exhibit substantial misunderstanding and miscommunication. For example, IT respondents said that "improving management insight into risk/compliance" was the most frequent objective for their IT GRC efforts, and business respondents said that this objective was the top benefit they could receive from IT GRC programs. However, both IT and business respondents listed efforts to improve management insight as one of their IT GRC program's areas of least success.

Differences in perceived potential value, priorities, and success will be roadblocks to what are otherwise successful IT GRC practices. Based on the results of our survey, it's clear that IT risk and compliance professionals need to:

- **Get more input from the business to align IT GRC with expectations.** Business and IT risk and compliance respondents who reported more frequent meetings had a better overall impression of the relationship between the two groups. The preferred method of meeting was to have a liaison from business join IT risk and compliance meetings. Furthermore, the two sets of respondents disagree almost completely on which IT GRC initiatives are most important based on current trends. Not only does increased meeting frequency correlate to a more positive perspective on the relationship, but it is also likely to help participants agree on objectives and priorities.

- **Focus more attention on efficiency and cost reduction.** The biggest issue business respondents had with IT GRC programs was the added cost impact on the company. Business respondents also said that considering current business trends, cost cutting should be the area of greatest focus in the near future. Meanwhile, IT respondents rarely listed cost-cutting as a priority for current IT GRC efforts and thought that cost-cutting was one of the least important areas to focus on given current business trends. While most IT GRC may include strong consideration for improved efficiency and lower costs, it needs to be seen more clearly as a priority on all projects.
- **Explain efforts more effectively to demonstrate value.** Most importantly, professionals responsible for IT GRC projects need to get better at explaining the value and success of their efforts. Given the perceived value of “improving management insight” and the amount of focus IT has on this goal, the fact that it was listed as one of the areas of least success suggests that expectations are either not clear or not realistic. In another discrepancy, business respondents placed “business continuity/disaster recovery” as the area where they would most like to see improvement from a knowledge management standpoint; however, the same group saw relatively little potential value in related GRC efforts such as “improving IT availability.” Explaining projects in terms that match business expectations and agreeing on success metrics will more effectively demonstrate the value of IT GRC programs.

## IT Risk And Compliance Programs Face Mounting Challenges

IT risks and regulations are not new. IT professionals have long been called upon by corporate compliance, legal, risk management, and other business functions to create, enforce, and report on a wide range of controls. Regulations like Sarbanes-Oxley elevated the visibility of IT control necessity to the top levels of the organization, while massive data breaches and outages marked the reality and potentially devastating impact of IT risks.

What is new is the number of risks and regulations IT is expected to address. IT risk and compliance professionals are working harder than ever to meet increasingly difficult challenges caused by:

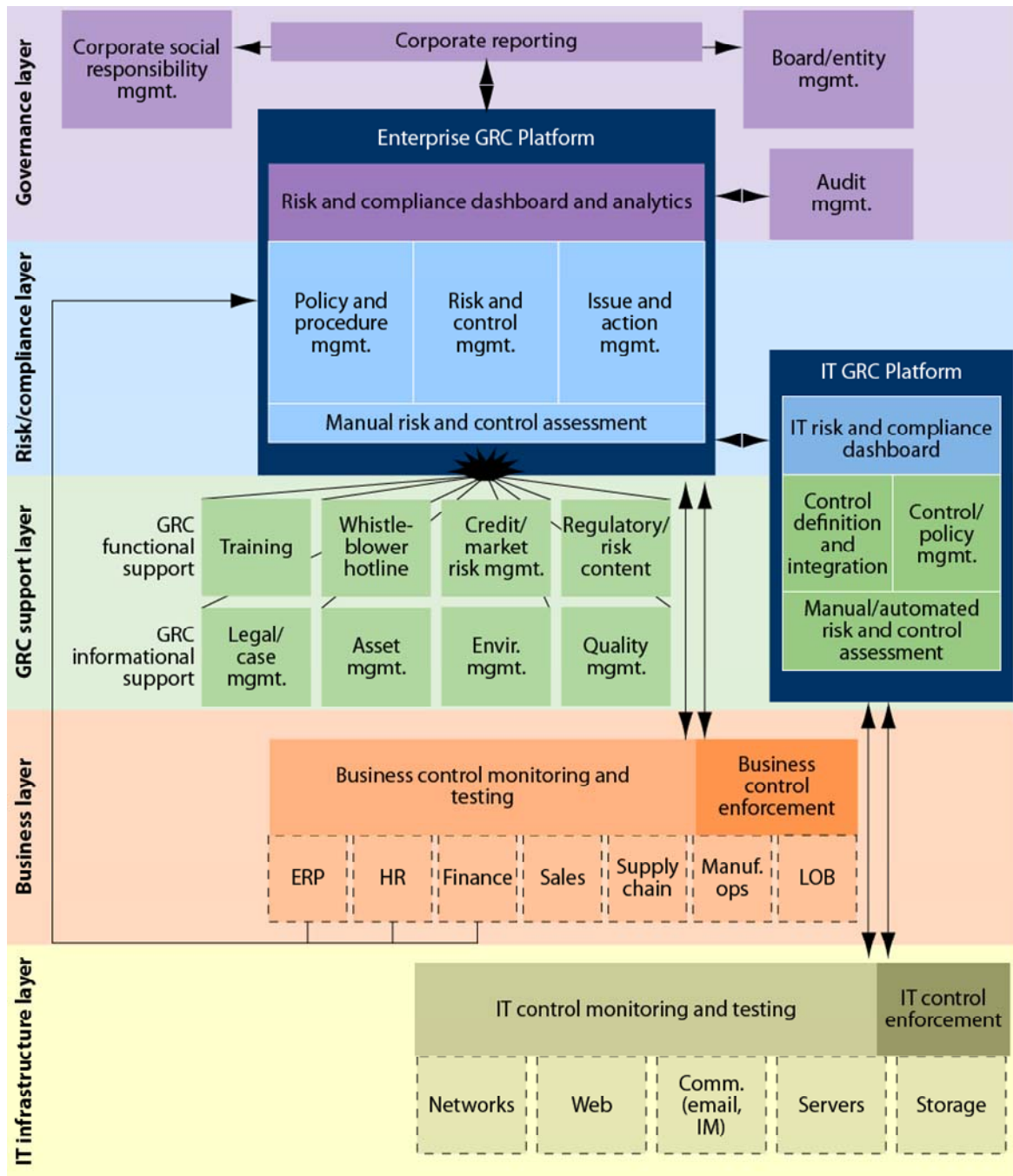
- **A more complex business environment.** The pace of business change is increasing. Reactions to global competition and economic difficulties result in more complicated partner relationships, overnight mergers and acquisitions, a globally distributed workforce, and greater reliance on IT service delivery. This means companies are operating under more regulatory jurisdictions and have partner requirements to address as well. Greater reliance on IT availability also means that the business impact of IT risks is compounded.
- **A more complex technology environment.** To keep up with business changes and an ever-changing workforce, IT is expected to introduce new and sometimes untested technologies in a drive to increase efficiency. These new products often create a larger threat profile and present challenges in control design and enforcement. IT is also faced with the seemingly impossible tasks of trying to assure the security of data and assets that may not always be within the confines of their IT environment.
- **Greater expectations that risks are appropriately managed.** Regulations worldwide continue to put more pressure on organizations to enforce greater control among their people, processes, and technologies. Regulators, credit rating agencies, business partners, investors, customers, and employees are no longer content with assuming a company is looking out for their best interests. They want to see reports and assurance.

## IT GRC Is Key To Meeting Business Needs

Scaling back the speed of business and refusing to adopt new technologies to support the business are rarely viable options. Similarly, failing to address business partner or regulatory requirements is not a choice that will be tolerated by most organizations.

Instead, IT departments are working to better organize their risk and compliance efforts to meet growing business needs. Many are establishing IT GRC programs, which coordinate key elements of risk and compliance programs in order to achieve greater efficiency and oversight. In many cases, this will include the implementation of software applications that facilitate or automate key GRC processes. A vast array of software vendors market IT GRC products, some of which help monitor or enforce controls within the IT infrastructure, while others help users manage IT GRC workflow, data collection, and reporting. Another set of vendors provide similar control management or program management capabilities for business processes and applications as well. Finally, there are vendors that provide products relevant to GRC as either supporting technologies (e.g., compliance training, asset management, incident response) or governance technologies (e.g., audit management, performance management). These products all exist within a very complex technology ecosystem (see Figure 1).

Figure 1: The GRC Technology Ecosystem



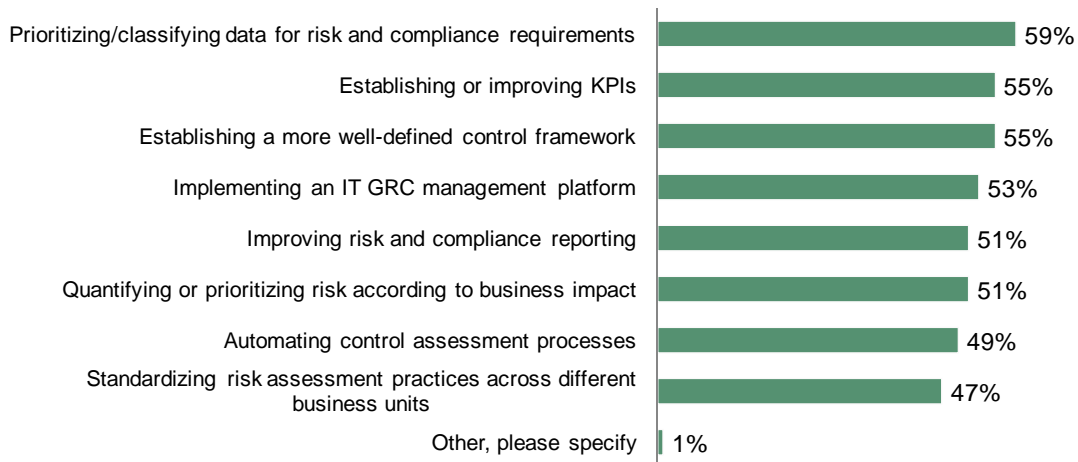
Source: February 3, 2009, "The GRC Puzzle: Getting All The Pieces To Fit" Forrester report

While organizations continue to demonstrate substantial value with GRC technology implementations, GRC itself is foremost an issue of process and strategy. Risk and compliance professionals must establish a method by which their efforts will be coordinated, who will be involved, and what they hope to accomplish. A governance structure must be established as well to set objectives and make ongoing progress toward achieving them.

IT GRC programs are going to look very different depending on the organization. However, many of them exhibit common initiatives. Prioritizing and classifying data for risk and control requirements was the most common IT GRC priority for the next 12 months among IT respondents, followed closely by establishing or improving key performance indicators (KPIs) and establishing a more well-defined control framework. Automating control assessment processes and standardizing risk assessment practices were the two least common priorities, but they still were on the priority list for nearly half of IT respondents (see Figure 2).

**Figure 2: Prioritizing/Classifying Data Tops This Year's GRC Priority List**

What are the top IT risk and compliance priorities for your organization in the next 12 months? (select all that apply)

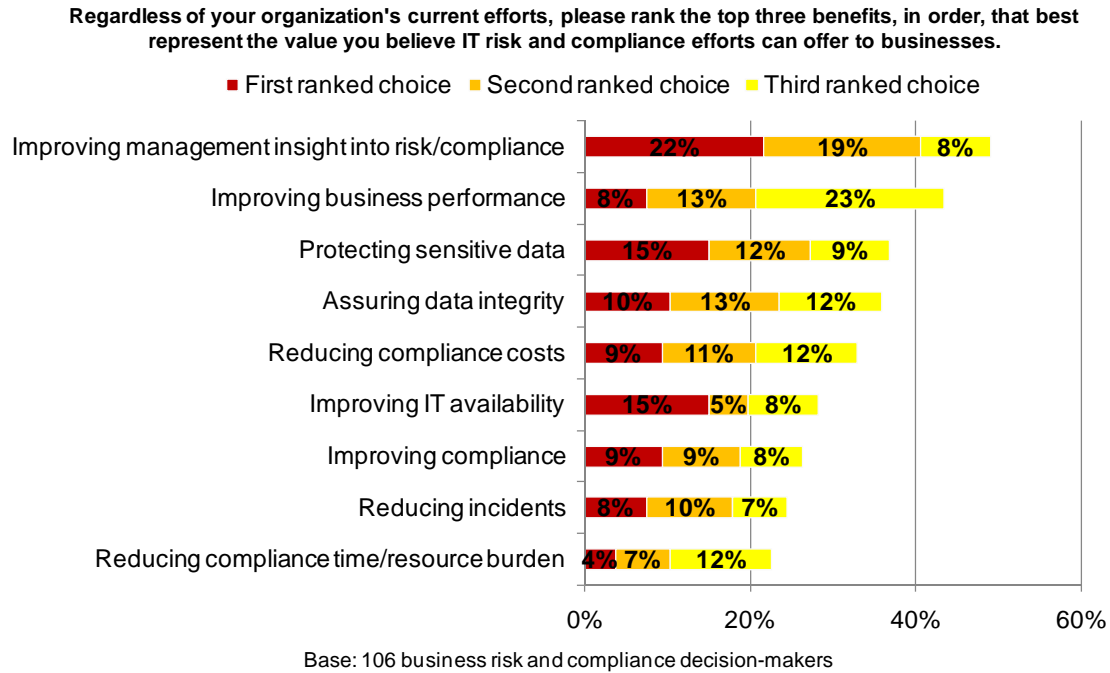


Base: 116 IT risk and compliance decision-makers

Source: "GRC: Business and IT Perspectives," a commissioned study conducted by Forrester Consulting on behalf of EMC Consulting, May, 2009

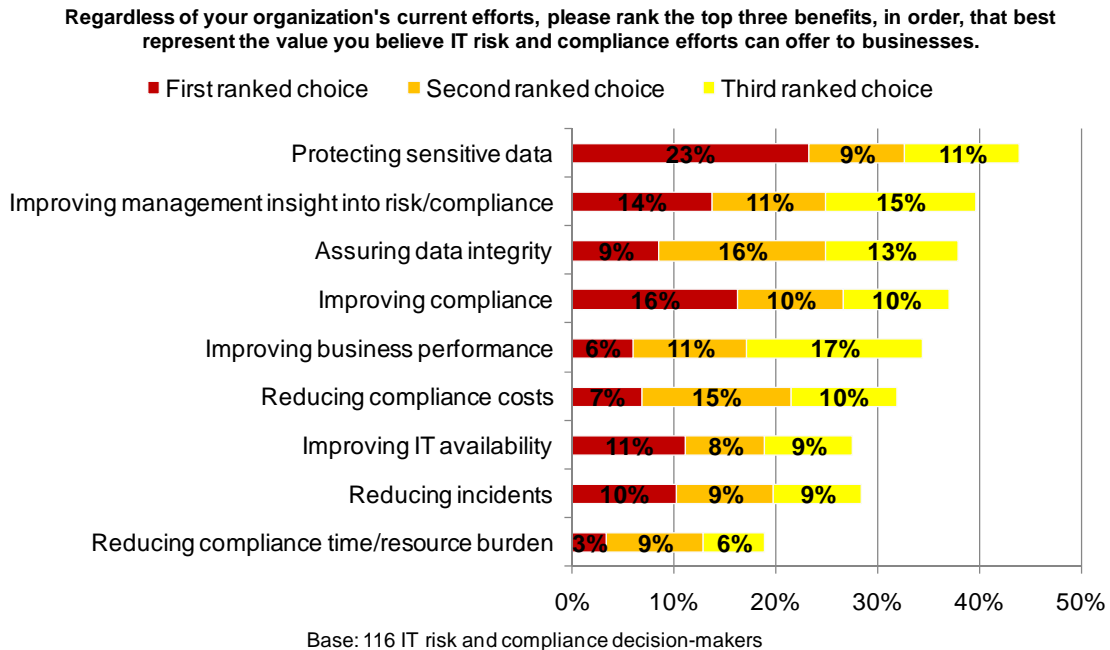
The two primary benefits of IT GRC programs are generally improved efficiency and increased oversight. However, when looking at a more granular level, business and IT professionals do not agree on the most important benefits that can be gained by IT GRC investments (see Figure 3 and see Figure 4).

Figure 3: Business View Of GRC Benefits



Source: "GRC: Business and IT Perspectives," a commissioned study conducted by Forrester Consulting on behalf of EMC Consulting, May 2009

Figure 4: IT View Of GRC Benefits



Source: "GRC: Business and IT Perspectives," a commissioned study conducted by Forrester Consulting on behalf of EMC Consulting, May 2009

## What The Business Doesn't Understand About IT GRC

---

There are some commonalities between business and IT respondents on their first choice of what value IT GRC can offer the business — most notably, the ability to improve management insight into risk and compliance. Looking at the overall rankings, however, there are larger discrepancies, such as ranking the ability to improve business performance (second highest ranked for business, fifth highest ranked for IT).

There may be several explanations for why discrepancies exist between the viewpoints of business and IT professionals on the values, priorities, and successes of IT GRC. It's possible that business professionals don't understand the work that goes into priorities such as protecting sensitive data. It's also possible that IT professionals spend their time delivering results from which business professionals get no value. In either case, IT professionals need to change their approach to IT GRC or risk alienating the business professionals who rely on them.

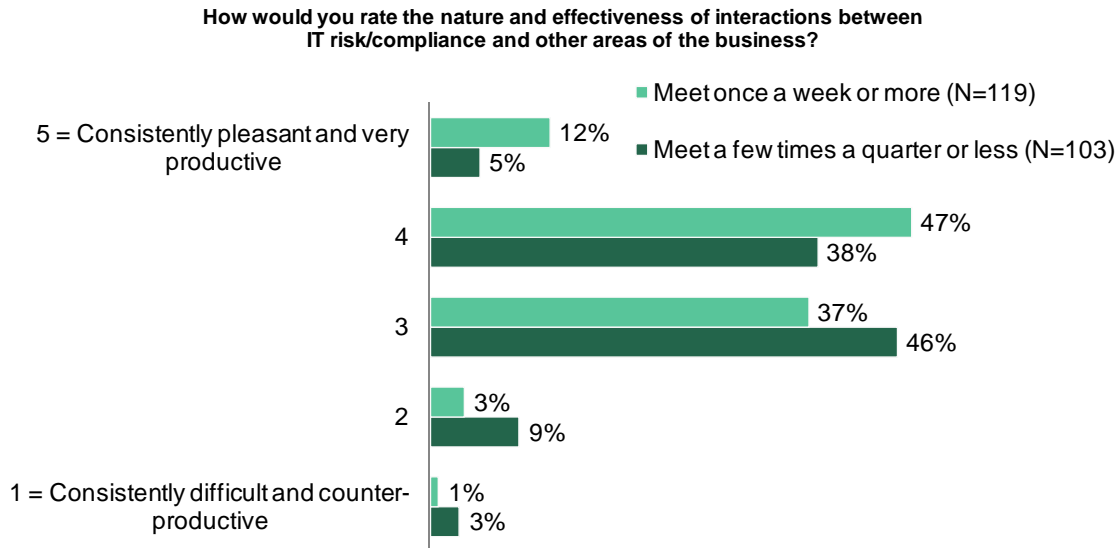
## IT GRC Alignment Needs Some Adjustment

Gaps between business expectations and IT performance in GRC are not necessarily a matter of poor performance or lack of budget. IT GRC professionals overall simply need to do a better job of making sure their efforts and explanation of their efforts are more closely aligned with business expectations. Based on the survey data, there are three primary aspects that require additional focus.

### IT Requires More Perspective From The Business

Taking all respondents into account, those who met more frequently with their counterparts had a more positive perception of the relationship than those who met less frequently (see Figure 5).

**Figure 5: Those Who Meet More Often Have A Better View Of Interactions Overall**



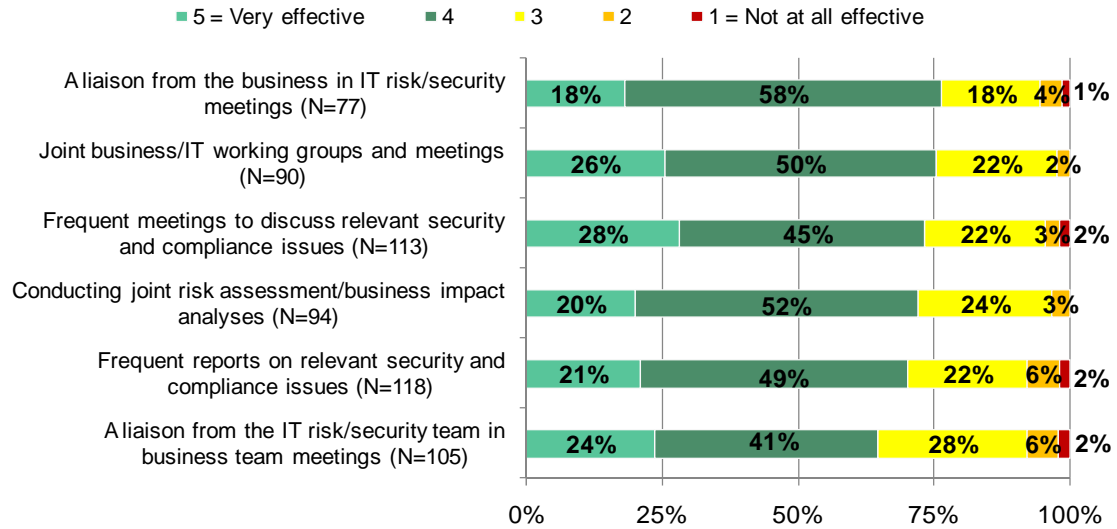
Base: risk and compliance decision-makers indicating either frequency of meetings between IT and the business

Source: "GRC: Business and IT Perspectives," a commissioned study conducted by Forrester Consulting on behalf of EMC Consulting, May 2009

How this interaction takes place is also important. While there are many ways collaboration might take place between business and IT risk and compliance professionals, survey respondents overall preferred to have a business liaison joining IT meetings (which is also the top preferred method of IT professionals and second most preferred method for business professionals). Creating joint working groups of both business and IT professionals was the second most preferred method of collaboration, and the method of choice for the business users. Note that having an IT liaison attend business meetings was the least preferred method overall (see Figure 6).

**Figure 6: A Business Liaison In IT Meetings Is Seen As The Most Effective Collaboration Method**

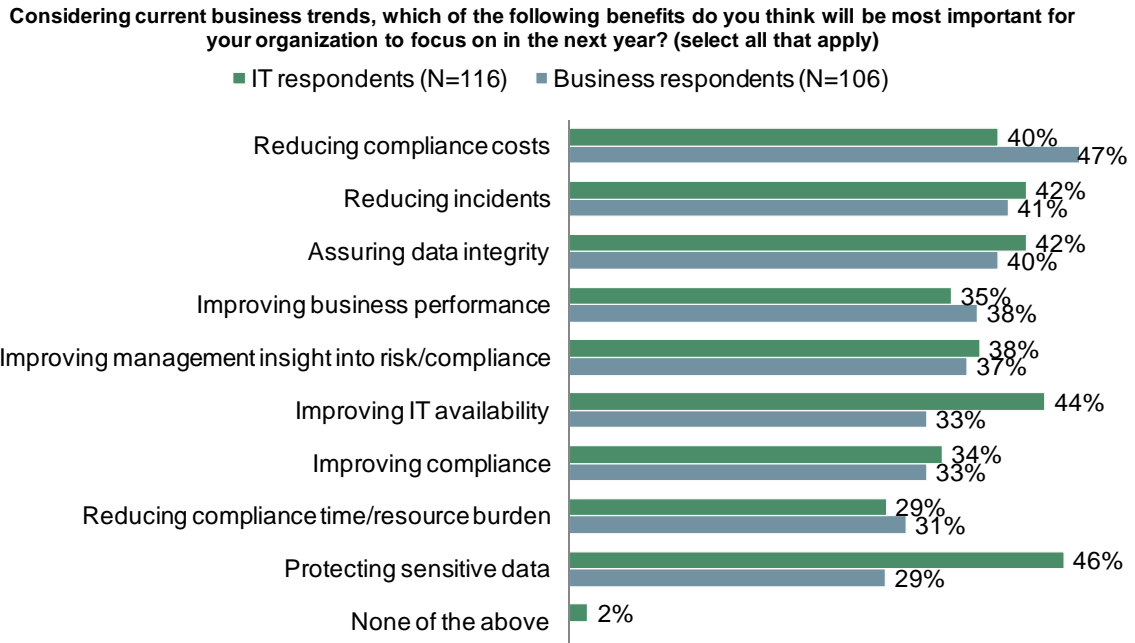
For each effort currently employed for increasing collaboration/communication, how effective is each in establishing a better working relationship between IT risk/compliance teams and other areas of the business?



Base: business and IT risk and compliance decision-makers indicating use of each collaboration method  
 Source: "GRC: Business and IT Perspectives," a commissioned study conducted by Forrester Consulting on behalf of EMC Consulting, May 2009

Finally, more frequent meetings will help align IT risk and compliance priorities with those of the business to help assure that projects meet expectations as much as possible. Current projects seem to be aligned with expectations, but when asked what IT risk and compliance professionals should be focusing their attention on over the next year given current business trends, there was a clear difference of opinion. IT respondents stated that their top priorities should be protecting sensitive data and improving IT availability, which were both at the very bottom or near the bottom of business respondents' priorities (see Figure 7).

Figure 7: Differing Perspectives On Upcoming Priorities



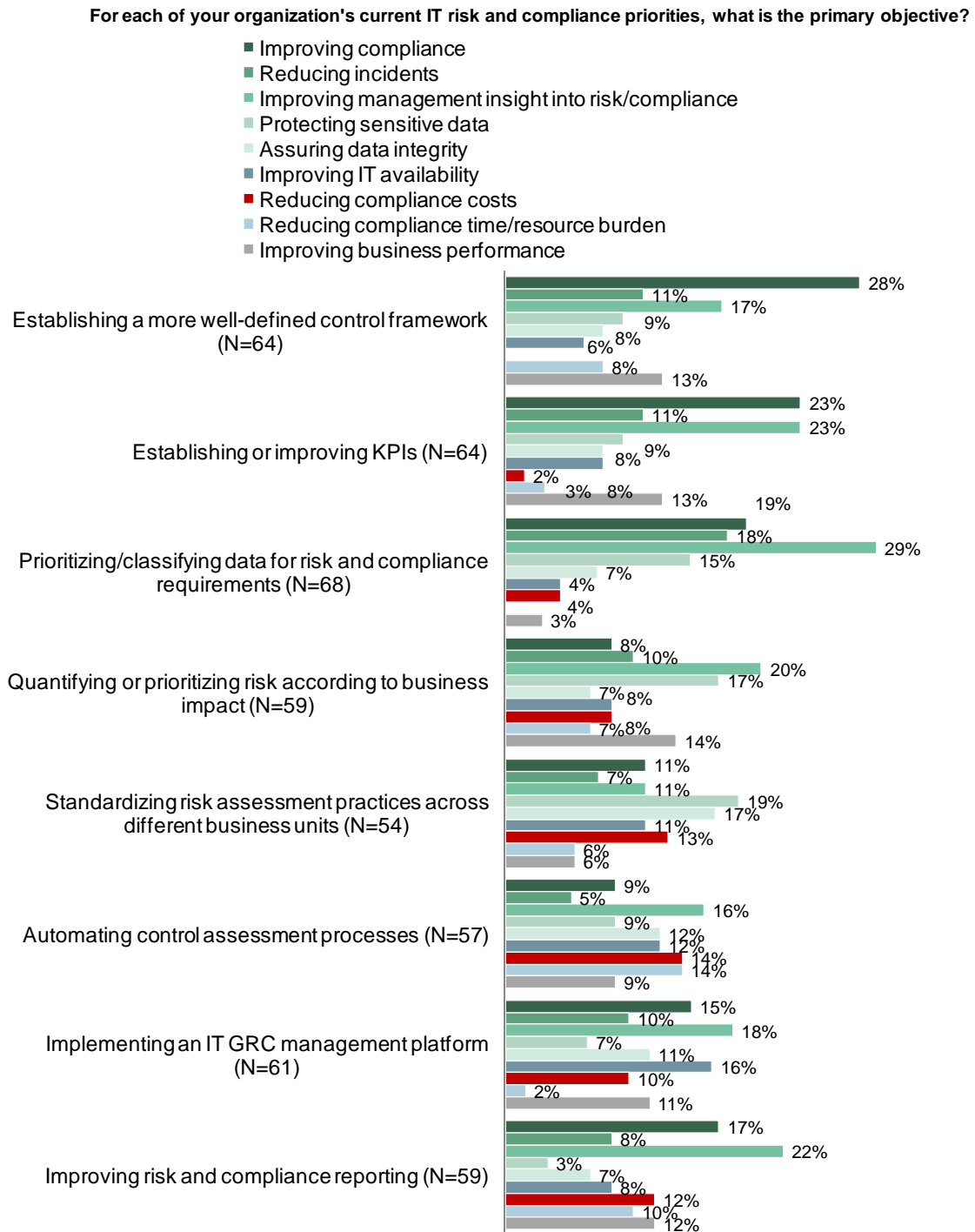
Base: risk and compliance decision-makers in either role

Source: "GRC: Business and IT Perspectives," a commissioned study conducted by Forrester Consulting on behalf of EMC Consulting, May 2009

### Cost Continues To Be A Major Business Concern

It is clear that business professionals see cost reduction as the most important priority to focus on given current business trends — a priority that only made the top five for IT risk and compliance professionals. A closer look at what IT risk and compliance professionals consider to be the objectives for their current IT GRC initiatives also shows that reducing costs is not high on the list, only occasionally named among the top three objectives for any project (see Figure 8). Variation is understandable, but the IT GRC projects in question showed very little consistency in their objectives and even less focus on addressing the chief concern among business respondents.

Figure 8: Cost Is Not High On IT's List Of Current GRC Objectives



Base: 116 IT risk and compliance decision-makers indicating each top GRC priority

Source: "GRC: Business and IT Perspectives," a commissioned study conducted by Forrester Consulting on behalf of EMC Consulting, May, 2009

IT professionals need to realize how important it is to consider cost-cutting as a top objective for their IT GRC projects. Even if costs are reasonable, business professionals see costs as their most difficult challenge by far when it comes to working with IT (see Figure 9).

**Figure 9: Business' Biggest Challenge In Working With IT: Increasing Costs**



Base: 106 business risk and compliance decision-makers

Source: "IT GRC: Business and IT Perspectives," a commissioned study conducted by Forrester Consulting on behalf of EMC Consulting, May 2009

If costs cannot be cut from IT risk and compliance programs, then it's incumbent upon IT to explain that they are considering cost reduction as much as possible, in addition to explaining the value achieved from any investments.

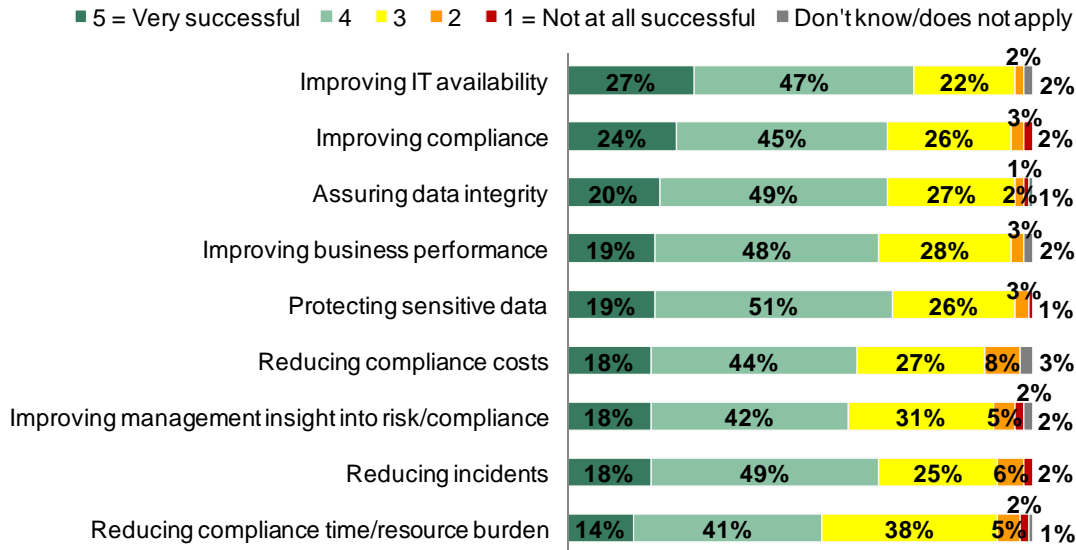
## IT Does Not Effectively Communicate Its Value

One of the trends we saw throughout the survey results was an apparent misunderstanding between IT and business respondents over what was actually occurring with regard to their IT risk and compliance efforts. This is not unexpected, as the universe of IT risk and compliance is extremely complicated and is not among the most important things for business professionals to understand. However, when it comes to the priorities of IT risk and compliance programs and the value that they are able to deliver, IT must do a better job translating the complexities of their efforts into business value.

As shown in Figure 2, business respondents consider IT GRC's top value to the business to be its ability to improve management insight into risk and compliance. As shown in Figure 7 and Figure 8, most IT GRC projects had improving management insight as the top objective. Despite that level of commitment, both IT and business respondents considered efforts over the last year to improve insight as one of the least successful areas in IT GRC (see Figure 10 and Figure 11).

Figure 10: Business View: Success Of GRC Efforts

To the best of your knowledge, please indicate the relative success of your organization's IT risk and compliance efforts over the last year in the following areas. (rank on a scale from 1 to 5, where 1 = not at all successful and 5 = very successful)



Base: 106 business risk and compliance decision-makers

Source: "GRC: Business and IT Perspectives," a commissioned study conducted by Forrester Consulting on behalf of EMC Consulting, May 2009

Figure 11: IT View: Success Of GRC Efforts

To the best of your knowledge, please indicate the relative success of your organization's IT risk and compliance efforts over the last year in the following areas. (rank on a scale from 1 to 5, where 1 = not at all successful and 5 = very successful)



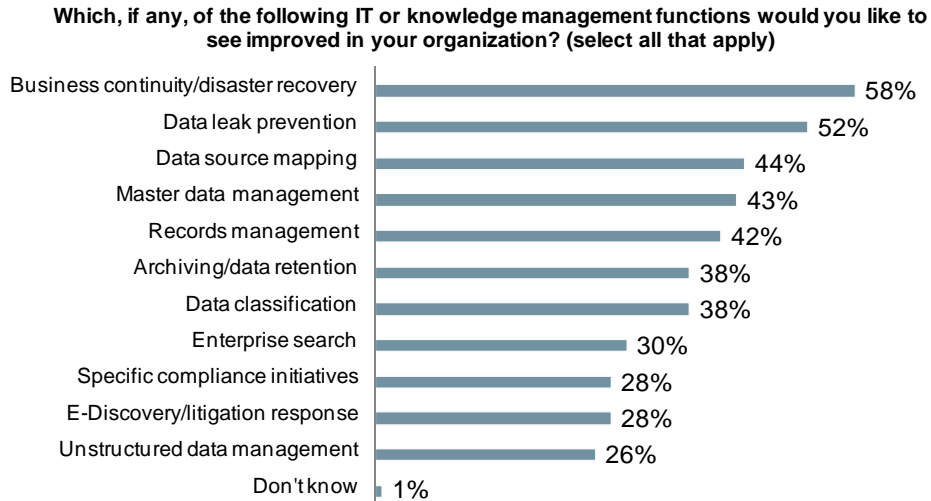
Base: 116 IT risk and compliance decision-makers

Source: "GRC: Business and IT Perspectives," a commissioned study conducted by Forrester Consulting on behalf of EMC Consulting, May 2009

The relatively low success rating given by the respondents may have several explanations, but considering the perceived value and the commitment of effort, it's a problem that needs resolution. IT risk and compliance professionals need to establish a set of success metrics with their business counterparts for objectives such as this. Understanding exactly what level of insight and what supporting data the business expects from IT will be critical.

One method IT risk and compliance professionals may find successful is to follow the lead of other areas' projects that have a more established connection to business expectations. With few exceptions, the knowledge management improvements that business professionals would most like to see align very well with the knowledge management initiatives that IT is currently undertaking (with the exception of IT involvement in data classification initiatives) (see Figure 12 and see Figure 13).

**Figure 12: Business Is Looking For Knowledge Management Improvements**

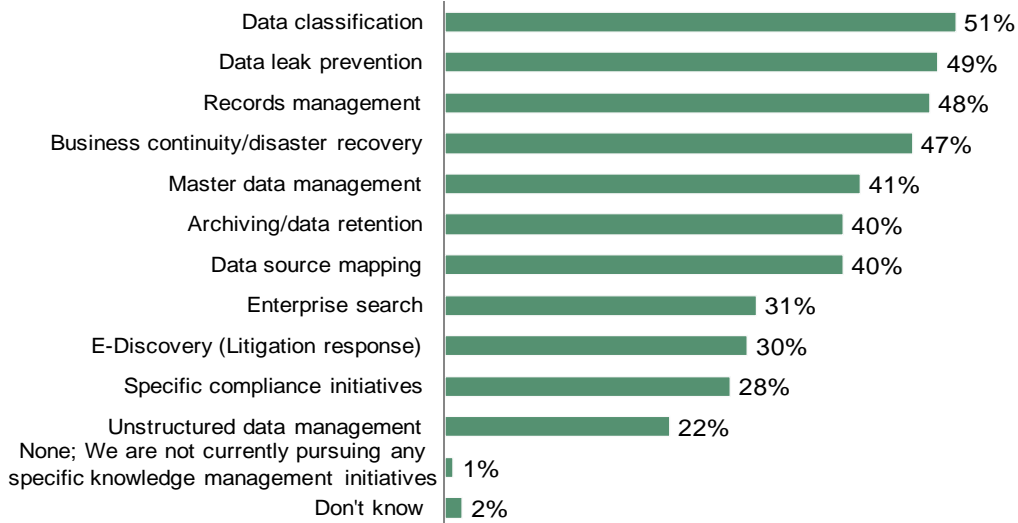


Base: 106 business risk and compliance decision-makers

Source: "GRC: Business and IT Perspectives," a commissioned study conducted by Forrester Consulting on behalf of EMC Consulting, May 2009

Figure 13: Current Knowledge Management Efforts Being Pursued By IT

Which, if any, of the following knowledge management initiatives is your organization currently pursuing?  
(select all that apply)



Base: 116 IT risk and compliance decision-makers

Source: "GRC: Business and IT Perspectives," a commissioned study conducted by Forrester Consulting on behalf of EMC Consulting, May, 2009

There is an additional benefit here, as many of the knowledge management initiatives that are high on the priority list for both IT and business are also the ones that are most connected to IT GRC efforts (see Figure 14).

Figure 14: Knowledge Management Initiatives Connect To GRC

Which of your IT or knowledge management initiatives are directly related to your IT risk and compliance initiatives?



Base: 116 IT risk and compliance decision-makers

Source: "GRC: Business and IT Perspectives," a commissioned study conducted by Forrester Consulting on behalf of EMC Consulting, May, 2009

## Recommended Steps Toward Improvement

IT professionals should take heart that their efforts are seen as important and valuable to business professionals. Where previously there has been a distinct divide between the two groups and little understanding between them, the changing nature of the corporate environment is creating opportunities for understanding and collaboration. Ongoing risk and compliance concerns regarding privacy, fraud prevention, business continuity, intellectual property protection, and other top enterprise risk and compliance concerns will continue to put more pressure on IT. They will also, however, offer IT the chance to elevate their service and value to the business.

As IT risk and compliance professionals work to coordinate their efforts into structured IT GRC programs, it is essential for them to address the priorities and concerns of the business. Along those lines, it is recommended that IT risk and compliance professionals:

- **Get more input from the business to align IT GRC with expectations.** Plan to meet every week or two with business counterparts to determine what the key priorities are for the business as a whole. Make sure to understand what the perceived value is from IT GRC projects and set expectations appropriately. Involving a business liaison in IT meetings is the preferred approach, but creating joint IT/business working groups shows favorable response as well. Use meetings to set project plan details and offer insight on status of key IT GRC initiatives and performance indicators.
- **Focus more attention on efficiency and cost reduction.** Efficiency is generally one of the most common benefits of GRC. However, regardless of how efficient IT GRC programs are or how much efficiency they create, business professionals see cost as the biggest concern by far when working with IT risk and compliance. For all IT GRC projects, clearly articulate to the business what is being done to minimize costs during implementation as well as on an ongoing basis. Part of this discussion should include an explanation that efforts to manage risk exposure and improve compliance can provide considerable return on investment.
- **Explain efforts more effectively to demonstrate value.** Risk and compliance efforts are among the most difficult and complicated aspects of IT, and business will continue to have a hard time understanding their real value. Determine at the beginning of projects what metrics will be used by IT and business to measure success. Certain objectives such as “improving management insight” are likely too vague to have concrete success metrics compared to “improving IT availability.” Make sure to use performance metrics that are directly impacted by the IT GRC program. In addition to cost reduction, focus on ways IT GRC projects can help improve business performance.

IT GRC programs are still relatively new, but they have already shown great success and even more promise in many organizations. Working to align efforts with business expectations will help assure IT that projects aren't perceived to be wasted efforts, helping solidify the collaboration and support that is required from the business in order to achieve ongoing success.

## Appendix A: Methodology

In this study, Forrester conducted an online survey of 222 large enterprises across multiple verticals in the US to evaluate GRC priorities of both business and IT professionals and how the two groups connect (and diverge) on this topic. Survey participants included 116 IT and 106 business decision-makers, all with direct responsibility or influence over one or more aspects of their organization's GRC efforts and strategy. Questions provided to the participants asked about their IT/business collaboration efforts, current GRC priorities/initiatives, the benefits/successes of GRC initiatives, and their view on future GRC strategy. The study was conducted in May 2009.