2008 Annual Report

IT Governance, Risk, and Compliance

Improving business results and mitigating financial risk
## Contents

**Executive summary** ................................................................. 1  
**IT GRC, business results, and GRC capability maturity** .............. 2  
**IT GRC among the most mature** ............................................. 3  
**An empirical IT GRC capability maturity model** ......................... 4  
**Implications and analysis** .................................................... 4  
**Key recommendations for action** ............................................ 5  
**What is IT GRC?** ................................................................. 7  
**Safely managing the speed of IT** ........................................... 8  
**The business impact of IT GRC maturity** .................................. 9  
**Business results: Customers, revenues, expenses, and profits** ........ 11  
**Loss or theft of sensitive data and IT GRC maturity** .................... 13  
**Regulatory compliance deficiencies and IT GRC maturity** .............. 15  
**Business downtime from IT service disruptions** ........................ 16  
**IT GRC maturity, financial rewards, and risks** .......................... 17  
**Business pressures impacting IT** ............................................ 18  
**Business and financial risks** ............................................... 19  
**Financial risk from the loss or theft of customer data** .................. 20  
**Financial risk from business disruptions due to IT service disruptions** 22  
**IT GRC: IT governance, risk, and compliance management** .......... 24  
**Organizational competencies and IT GRC maturity** ..................... 25  
**Who should be involved in IT governance** ............................... 25  
**Who should be involved in assessing and demonstrating compliance** 27  
**Employee training: A culture of compliance** ............................ 28  
**Organizational actions to improve IT GRC results** ...................... 29  
**Business risks, assessments, and priorities** ............................. 30  
**IT GRC functions and practices** ............................................ 31  
**Framework usage and IT GRC maturity** ................................... 32  
**Measurable results, Continuous Quality Improvement, and IT GRC** .... 34
Executive summary

Managing the value delivered by IT is traditionally associated with managing change to business procedures and applications that directly impact customer retention, sales, revenues, profits, and expenses.

Although valid, this view as the sole way to measure the value of IT is under siege as more organizations experience increasing loss or theft of customer data and endure the fallout from these events, including customer defections, revenue losses, declines in public capitalization, increases in expenses, and short-term profit declines. Not limited to managing and protecting customer data, IT is being challenged to maintain nearly 100 percent uptime to avoid business disruptions while cost-effectively responding to numerous legal requests, statutes, and regulatory audits.

In today’s global economy, the livelihood of the organization is linked to how well the IT function manages the availability, integrity, and confidence of the information and IT systems used to operate core business procedures. Whether it is protecting information or meeting legal and regulatory requirements, the challenge confronting IT managers in an increasingly interconnected world means managing business opportunity and risk simultaneously.

The most recent research conducted by the IT Policy Compliance Group shows that improvements to data protection and compliance are paying big dividends among firms with the most mature governance, risk management, and compliance management practices. These include:

- Consistently higher revenues than all other firms
- Much higher profits than all others
- Better customer retention rates
- Dramatically lower financial risks and losses from the loss or theft of customer data
- Significantly reduced financial impact from business disruptions caused by IT disruptions
- Much lower spending on regulatory audit

Unfortunately, only slightly more than one in ten firms are enjoying the extraordinary business benefits associated with these most mature practices.

In contrast, about seven in ten organizations are experiencing business results that are half of what the leading firms deliver while also posting financial losses that are much higher. Moreover, most of these firms are overspending on regulatory compliance due to high use of manual procedures and less mature practices.

The worst performers, about two in ten organizations, are experiencing much lower business results than all other firms, much higher financial losses, and much more difficulty with regulatory and legal mandates.
What is striking from the research is the organizations with best business results are the same firms with the most mature practices. The converse is also true: the organizations with the worst business results are the same firms with the least mature practices. Defining IT GRC broadly as (1) the management of value delivered to the organization by IT; (2) the management of risk associated with the use and disposition of IT resources; and (3) the management of compliance with corporate policies, legal statutes, and regulatory audits, this annual report shines a spotlight on the competencies, capabilities, and practices that are most responsible for influencing and impacting business rewards and risks.

**IT GRC, business results, and GRC capability maturity**

Simply put, the more mature the practices for managing reward and risk, the better the business results of the organization and the lower the financial risks. Conversely, the less mature the IT practices, the worse the business results and financial losses (see Figure 1).

Firms with the most mature IT GRC practices experience, on average, 8.5 percent more revenue than those operating in the middle of the normative range. Compared to the least mature, the most mature firms are experiencing revenues that are 17 percent higher. Similar disparity in results for expenses in IT, profits for the firm, customer satisfaction, and customer retention show that the maturity of IT GRC practices for managing reward and risk has a direct impact on the organization.

<table>
<thead>
<tr>
<th>IT GRC Maturity</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Population</td>
<td>20%</td>
<td>68%</td>
<td>12%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer satisfaction</td>
<td>-8.7%</td>
<td>-4.4%</td>
<td>0%</td>
<td>4.4%</td>
<td>8.7%</td>
</tr>
<tr>
<td>Customer retention</td>
<td>-6.3%</td>
<td>-3.2%</td>
<td>0%</td>
<td>3.2%</td>
<td>7.3%</td>
</tr>
<tr>
<td>Revenue</td>
<td>-8.5%</td>
<td>-4.3%</td>
<td>0%</td>
<td>4.3%</td>
<td>8.5%</td>
</tr>
<tr>
<td>Expenses</td>
<td>-6.4%</td>
<td>-3.2%</td>
<td>0%</td>
<td>3.2%</td>
<td>6.4%</td>
</tr>
<tr>
<td>Profits</td>
<td>-6.9%</td>
<td>-3.5%</td>
<td>0%</td>
<td>3.5%</td>
<td>6.9%</td>
</tr>
<tr>
<td>Financial risk from customer data loss/theft</td>
<td>9.6% of revenue</td>
<td>8% of revenue</td>
<td>6.4% of revenue</td>
<td>3.2% of revenue</td>
<td>0.4% of revenue</td>
</tr>
<tr>
<td>Financial risk from disrupted business operations</td>
<td>10% of revenue</td>
<td>3% of revenue</td>
<td>1% of revenue</td>
<td>0.4% of revenue</td>
<td>0.2% of revenue</td>
</tr>
<tr>
<td>Spending on regulatory compliance</td>
<td>37% lower than maximum</td>
<td>3% lower than maximum</td>
<td>3% lower than maximum</td>
<td>20% lower than maximum</td>
<td>52% lower than maximum</td>
</tr>
</tbody>
</table>

Figure 1. Operating results and IT GRC maturity

*Source: IT Policy Compliance Group, 2008*
**IT GRC among the most mature**

Marked by a focus on operational excellence, firms with the most mature IT GRC profiles have established an integrated approach to managing risk and reward within the IT function and across the entire organization. Among these firms, senior managers in IT are employing the balanced scorecard to:

1. Regulate reward and risk decisions impacting the organization
2. Establish policies and objectives for IT
3. Institute a learning and growth culture that includes continuous quality improvement within the IT function (see Figure 2)

Within the IT function, and across legal, audit, internal controls, and business lines, the management of objectives for business reward and risk are being achieved with continuous quality improvement, control objectives, frequent measurement and reporting, common procedures, and high levels of automation, all complemented by IT service level objectives and contracts with IT vendors. Within the IT operations function, the focus is on common IT procedures, more automated controls, continuous measurement, and diligent IT change management and prevention procedures.

Marked by the use of Six Sigma among some firms and simpler Continuous Quality Improvement cycles among many others, the most mature organizations establish a focus on operational excellence within IT that reflects results back into the objectives established and improved through the use of a balanced scorecard. Among these firms, the hallmark of the approach is: Make it easy to understand, easy to implement, and continuously improved.

*Figure 2. IT GRC among the most mature*

*Source: IT Policy Compliance Group, 2008*
The Continuous Quality Improvement effort for the governance of IT and the balancing of reward and risk associated with the use of IT takes place at all levels within IT, and across the organization, among the most mature organizations.

**An empirical IT GRC capability maturity model**

Primary benchmark research conducted by the IT Policy Compliance Group during the past two years has resulted in a GRC Capability Maturity Model (GRC CMM) with specific practices, competencies, and capabilities associated with each maturity level. This fact-based GRC Capability Maturity Model can be used to assess current maturity levels and quantify the business outcomes associated with each maturity level, as well as identify desired business outcomes and the capabilities, practices, and competencies needed to improve results.

The scale employed for the GRC CMM borrows from prior research, including significant contributions made by ISACA and the IT Governance Institute. Against this scale, the business results, financial losses, financial risks, business disruptions, and regulatory compliance experience of more than 2,600 firms have been mapped, from worst (level 1) to best (level 5) results.

The competencies, capabilities, and practices associated with each maturity level in the GRC CMM are those of the firms with specific business results at each level. This basis for the practices, capabilities, and competencies in the GRC CCM delivers empirical insight into what is working and not working, based upon primary research and facts, not hypothesis.

**Implications and analysis**

The way to improve business results and to reduce risk, loss, and expense is to increase or enhance the IT GRC competencies, practices, and capabilities governing the business rewards and risks associated with the use and disposition of IT.

While most organizations will need to improve results, operating at the highest maturity level may be inappropriate for some firms. For some, the desired objective may be to operate at level 4.5 or 4.0 on the GRC CMM maturity scale. As a result, improving the balance between business reward and risk for a specific organization is going to be a journey that must be taken relative to the industry within which it competes.

**Organizational competencies**

The organizational competencies implemented by the most mature firms include leadership by IT, legal, audit and finance functions; employee training and a culture of compliance; improvements to specific practices and capabilities within IT operations; IT assurance and audit; and a continuous quality improvement effort. These are the hallmarks of an integrated IT GRC program being implemented by the most mature firms.
Practices and capabilities

In addition to organizational competencies, specific practices and capabilities leading to better business results and less financial risk, loss, and expense include segmenting and safeguarding customer data, rationalizing policies and control objectives, common procedures and systems, more controls, much more automation, change management, and continuous measurement, among others.

Key recommendations for action

Based on the relationship between the maturity of IT GRC practices among organizations and the business reward and risk outcomes being experienced by firms at different maturity levels, the key recommendations from the research include actions for senior managers, vice presidents, managers, and directors, as well as recommendations for use within IT operations, IT assurance, and IT audit.

Although the end goal for some firms may be to operate at the most mature levels for IT GRC, others may find this inappropriate. All firms will want to evaluate their specific financial rewards and risks when deciding which level of IT GRC maturity is desirable, and what improvements have to be made to achieve their objectives.

For this reason, it is important that managers first assess the maturity of their own organization; determine the optimal reward, risk, and expense targets; establish the desired level of maturity; and identify and implement the improvements needed to achieve their objectives.

After identifying objectives for important business metrics, the GRC CMM enables organizations to identify the following, based on targeted maturity levels:

- Increases in revenue, profit, and customer retention
- Avoidance or mitigation of financial and operational risk and loss
- Expense reductions for legal and regulatory compliance
- Practices and capabilities needed to achieve objectives
- Organizational competencies needed to achieve objectives
It is important to assess results, both before and after changes to practices, capabilities, and competencies within the organization. Only by measuring before and after will the organization know whether the improvements are sufficient or not.

This simple recipe for Continuous Quality Improvement supplies the backbone for a measurable and integrated IT GRC program within IT that will optimize the balance between reward and risk, as demonstrated by the results being achieved by the most mature organizations.

**Improving competencies, practices, and capabilities**

The capabilities, practices, and competencies directly associated with higher GRC CCM maturity levels provide the opportunity to diagnose specific shortfalls or misaligned activities that a firm may already have implemented (see Figure 3).

For instance, an organization may have implemented continuous monitoring but may find that its Continuous Quality Improvement program is based on vague or nonexistent metrics that stifle its progress. Or, a firm may find that it has implemented a balanced scorecard for the alignment of value delivered by IT without any of the underlying practices necessary to enhance IT GRC maturity.
Some organizations may find that moving from their current state of maturity will require an incremental approach through planned stages. In this case, it is critical to identify the shortfalls against benchmarked practices and capabilities and develop phased plans that are based on priorities to improve specific practices as part of a longer-term plan for improving results.

Assessing the current level of maturity and the desired objective, along with the practices and capabilities needed to improve results, can be accomplished with the assistance of this research report. The tables in Appendix A list specific business outcomes for each maturity level. Similarly, the practices, capabilities, and competencies correlated with each maturity level are listed in these tables. The current state of maturity, desired objectives, and specific practices that might be needed to improve results can also be found in the tables in Appendix A.

In addition, interactive assessment tools at the IT Policy Compliance Group website (www.itpolicycompliance.com) will provide an automated method to assess the current maturity of the organization, the business outcomes for each level of maturity, and the improvements that can be targeted.

**What is IT GRC?**

Simply, IT GRC encompasses the practices for delivering the following:

1. Greater business value from IT strategy, investment and alignment
2. Significantly reduced business and financial risk from the use of IT
3. Conformance with policies of the organization and its external legal and regulatory compliance mandates

While some of these practices involve continuous improvement to quality, others involve practices and capabilities that are known to be effective, along with objectives for what the organization wants to achieve. IT GRC energizes the entire organization to imagine what it can achieve, establishes methods for achieving their objectives, and demonstrates the practices that are proven to work for minimizing business and financial risk.

Fundamentally, IT GRC is about striking an appropriate balance between business reward and risk, enabling an organization to more effectively anticipate and manage business risk while more effectively delivering value for the organization (see Figure 4).
Safely managing the speed of IT

Much like a team trying to win an automobile race, an organization may choose to press the accelerator pedal of IT usage and change to the floor. But, when road conditions, fuel remaining in the tank, tire conditions, brakes, and drivers change, or when drivers are not paying attention, accidents are more likely to occur.

![Diagram of speed vs. risk]

Figure 4. Managing the speed of IT
Source: IT Policy Compliance Group, 2008

Objectives of organizations cannot be achieved when IT change does not keep pace with changing business conditions. Similarly, when the pace of IT change or use is faster, accidents are more likely. IT GRC involves the practices and procedures implemented to:

- Govern the investment and alignment of IT strategies and resources
- Manage risks associated with the introduction, use, and disposition of IT resources
- Manage compliance with company policy, regulatory, and legal requirements

Like the driver of an automobile, experience begets greater maturity, enabling some organizations to accelerate past competitors with less worry.
The business impact of IT GRC maturity

IT GRC maturity covered by this research report is based upon the following:
1. Primary research results conducted with thousands of organizations
2. The practices and capabilities directly related to business rewards and risks experienced by these firms
3. The practices and capabilities associated with each level of reward and risk
The result is a maturity matrix that is based upon empirical evidence (see Figure 5).

<table>
<thead>
<tr>
<th>IT GRC Maturity</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Population</td>
<td>20%</td>
<td>68%</td>
<td>12%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nonexistent practices and procedures</td>
<td>Initial ad hoc procedures and practices</td>
<td>Repeatable but intuitive procedures and practices</td>
<td>Defined procedures and practices</td>
<td>Managed and measured procedures and practices</td>
<td>Optimized and balanced procedures and practices</td>
</tr>
<tr>
<td>Business result metrics</td>
<td>Lowest results</td>
<td>Lowest to highest results</td>
<td>Highest results</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial impact from data loss or theft and IT service level disruptions</td>
<td>Highest financial risk</td>
<td>Highest to lowest</td>
<td>Lowest financial risk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT GRC business risk indicators</td>
<td>Highest</td>
<td>Highest to lowest</td>
<td>Lowest</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

N: 2,608

Figure 5. IT GRC maturity capability model
Source: IT Policy Compliance Group, 2008

The descriptions of the maturity levels for GRC in this report are similar to and borrow from much previous research, including contributions made by supporting members of the IT Policy Compliance Group, including the Computer Security Institute, the Institute of Internal Auditors, ISACA, the IT Governance Institute, Protiviti, and Symantec (see Appendix A).
However, after the scale and descriptions of the maturity levels, the findings contained in this report differ markedly from available maturity models in three principal ways, as follows:

1. The findings are focused exclusively on IT GRC.

2. The maturity described by the report is directly linked to financial results and risks from primary research benchmarks.

3. The practices and capabilities are directly related to business outcomes at each maturity level, based on primary research benchmarks.

There are many different maturity models available. Most provide a way to assess practices and capabilities needed to improve results for a specific purpose, along with a roadmap for evaluating current and desired future states. The maturity relationships contained in this report rely on benchmark findings and publicly available data for business outcomes, financial risks, and business risk indicators throughout the entire spectrum, from one end to the other. If a result, a practice or a capability is not grounded in the reality of actual experience, it is not contained in the report or the GRC CMM.

There are direct relationships between the maturity of IT GRC practices and capabilities, and the business results—positive and negative—being experienced by organizations. The primary IT GRC metrics tracked by the benchmarks include customer satisfaction, customer retention, revenue, profit, financial loss and the occurrence of such losses after the loss or theft of customer data, business disruptions leading to financial losses that are directly related to IT service disruptions, and the number of regulatory compliance deficiencies that must be corrected to pass audit and that are costing the organization more, or less, money to sustain regulatory audit results.

Results from the benchmarks consistently show a normal distribution of results for these metrics, from the worst business results to the best, from the worst financial losses to the best, from the most business disruptions to the least, and from the most difficulty with regulatory audit to the least. Consistently, within and across all of the benchmarks, the population with the worst results is 20 percent of the population of firms participating in the benchmarks, and those firms with the best results number 12 percent of the population. In between these two ends of the spectrum lies a majority of the population, 68 percent, with normative results: between the worst and the best.

This consistently normal distribution of results is accompanied by consistent research findings related to a number of factors, including:

• Actions being taken to improve results
• Competencies and capabilities to take these actions
• Practices implemented by organizations to take these actions

The consistency in business outcomes, aligned with consistent findings in the actions, competencies, capabilities, and practices forms the basis for the GRC CMM being covered in this annual report, focusing on IT GRC maturity.
Across more than 2,600 separate organizations, the findings show that roughly two in ten organizations are operating with worst business results and the highest business risks. The findings also show that a little more than one in ten organizations are posting the best business results and the least financial risk. In between these two are a majority of firms, with neither the best business results nor the worst financial losses (see Figure 6).

Figure 6. Distribution of business results by maturity
Source: IT Policy Compliance Group, 2008

Each of the metrics measured by the benchmarks shows results that are consistently repeated, including business results, financial risk from data loss or theft, business disruptions, and the experience that organizations are having with regulatory compliance.

**Business results: Customers, revenues, expenses, and profits**

The most recent benchmarks measure the impact that improvements to data protection, regulatory compliance, and IT service level resiliency have had on business results, including customer satisfaction, customer retention, revenue, expenses, and profits. Tracked on a 10-point scale and measured by percentage changes, the results show the same population distribution:

- Twenty percent of organizations have an overall score of 6.37 for these five business results, on the high-end of “no impact.”
- Sixty-eight percent of firms have an overall score of 6.86 for these five business results, on the low-end of a “slight increase.”
- Twelve percent of organizations have an overall score of 7.40, in the middle of the range for “slight increase.”
The raw scores clearly show that firms with better IT GRC results are enjoying much better results when it comes to satisfying customers, retaining customers, and growing revenues and profits than all other organizations (see Figure 7).

Although there is a slight improvement among all firms, the results show clearly that the most mature firms are experiencing much better business results.

Unfortunately, the average scores across these performance domains do not show the gulf separating the results between the organizations with the least and most mature IT GRC profiles. The percentage changes and relative scores provide much greater insight into the contribution to business results being achieved by firms with the most mature IT GRC practices.

**Business results: Relative to the norm**

Whether normalized to the mean scores for each business metric or measured directly from percentage changes that occurred for organizations, the change in value for customer satisfaction, customer retention, revenues, expenses, and profits shows a swing that ranges from nearly negative 10 percent on the low side among the least mature to nearly positive 10 percent on the high side being experienced by most mature firms, matching raw scores from other portions of the benchmarks (see Figure 8).

Although posting results that are on the high end of “no impact,” the majority of firms operating as least mature are experiencing results that are 7.4 percent less than that of the firms operating at the IT GRC norm for all business metrics.
The most mature firms, those posting results in the middle of “slight increase” for all business metrics, are experiencing results that are averaging 7.6 percent more than the firms operating at the norm for all business metrics.

The majority of firms—those operating at IT GRC norm—are not experiencing the more dramatic differences in revenues, expenses, profits, customer satisfaction, or customer retention being posted by the firms with the most, or least, mature IT GRC profiles, practices, competencies, and capabilities.

**Loss or theft of sensitive data and IT GRC maturity**

The loss or theft of sensitive data is another of several IT GRC business risk indicators tracked by the benchmarks. The population distribution for these metrics show:

1. Twenty percent of the population has the worst data protection results, with more than 12 losses or thefts of sensitive data each year.
2. Sixty-eight percent of the population has normative data protection results, with between 3 and 12 losses or thefts of sensitive data annually.
3. Twelve percent of the population has the best data protection results, with fewer than 3 losses or thefts of sensitive data each year.
Data theft or loss and IT GRC maturity correlation: Same firms dominate

In addition to the population distribution, the set of organizations that compose each of the major areas (least mature, normative, and most mature) is almost identical, with slight variations. For example, 75 percent of the firms with the least mature IT GRC results are the same firms with the largest and most frequent losses or thefts of sensitive data. Almost all—92 percent—of the firms with middling IT GRC results are the same firms with somewhere between 3 and 12 losses or thefts of sensitive data each year. And, nearly all—96 percent—of the firms with the best IT GRC results are the exact same firms with the fewest and least frequent losses or thefts of sensitive data annually (see Figure 9).

The alignment of the findings raises some interesting questions, such as:

• Is information more secure because of better regulatory compliance practices?
• Do better data protection practices deliver better customer satisfaction, retention, revenue, and profits?
• Are more mature results for IT GRC related to better business results, better data protection, and regulatory compliance results?
Regulatory compliance deficiencies and IT GRC maturity

Regulatory compliance results are but one of several IT GRC business risk indicators tracked by the benchmarks. The population distribution for these metrics show:

1. Twenty percent of the population has the worst regulatory compliance results, with more than 12 deficiencies that must be corrected to pass audit.
2. Sixty-eight percent of the population has normative regulatory compliance results, with between 3 and 12 deficiencies that must be corrected to pass audit.
3. Twelve percent of the population has the best regulatory compliance results, with fewer than 3 deficiencies that must be corrected to pass audit.

*Least mature = worst compliance results; most mature = best compliance results*

In addition to the population distribution, the organizations that compose each of the major areas (least mature, normative, and most mature) demonstrate alignment of results by maturity. For example, 76 percent of the firms with the least mature IT GRC results are the same firms with the most audit deficiencies that must be corrected to pass audit (see Figure 10).

![Figure 10. Regulatory compliance results](source: IT Policy Compliance Group, 2008)
Almost all—93 percent—of the firms with middling IT GRC results are the same firms with somewhere between 3 and 12 audit deficiencies that must be corrected to pass audit. And, nearly all—97 percent—of the firms with the best IT GRC results are the same firms with the least number of regulatory audit deficiencies that must be corrected to pass audit.

**Business downtime from IT service disruptions**

Very similar results are posted for business disruptions due to IT service disruptions, many of which are due to IT security events. Roughly 20 percent of all firms suffer the highest levels of downtime: more than 80 hours annually. Another 68 percent are operating somewhere in the middle, with between 2 and 80 hours of downtime each year due to IT disruptions. And, only 12 percent are fortunate enough to have business operations halted for 2 hours or less each year due to IT disruptions.

*Business downtime and IT GRC maturity correlation: Same firms dominate*

The majority—80 percent—of organizations with the least business downtime from IT service disruptions are the same firms with the least data loss or theft and the fewest regulatory compliance deficiencies to correct. A majority—63 percent—of the firms with the most stagnant business results are the same firms with the most business downtime from IT disruptions, the largest number of regulatory compliance deficiencies, and the most loss of sensitive data. Lastly, 78 percent of the firms with annual hours lost to IT service disruptions are the same firms with normative results for all of the metrics (see Figure 11).

![Percentage of organizations](image)

**Figure 11. Business downtime from IT service disruptions**

*Source: IT Policy Compliance Group, 2008*
The alignment of the findings raises an interesting question: What are the IT GRC practices that translate into improved business results, including higher revenue, better profits, better customer retention, and improvements in IT service reliability, as well as better regulatory compliance results and less frequent loss of sensitive data?

**IT GRC maturity, financial rewards, and risks**

All of the business and financial rewards, and all of the financial and operating risks from the benchmarks, are aligned with IT GRC maturity among firms (see Figure 12).

![Figure 12. Alignment of IT GRC maturity with business rewards and risks](source: IT Policy Compliance Group, 2008)

The majority of the firms that are least mature when it comes to IT GRC are experiencing the worst business results, the most financial risk from data loss or theft, the highest financial losses from IT-based business disruptions, and the worst regulatory compliance results.

In contrast, the majority of firms with the most mature IT GRC profiles are the same firms experiencing the best business results, the least financial losses from data loss or theft, the lowest financial risk from IT-based business disruptions, and the least number of problems with regulatory compliance. Lastly, the majority of the firms operating in the norm are experiencing financial results that are between those of the firms with the least mature and most mature IT GRC profiles, practices, capabilities, and competencies.
Business pressures impacting IT

The business pressure that most impacts IT among all organizations is the protection of sensitive data. This includes customer data, employee data, corporate data, and IT security- and audit-related data (see Figure 13).

![Figure 13. Primary pressures impacting IT](source: IT Policy Compliance Group, 2008)

After protecting sensitive data, the pressures most impacting the use of IT include:

- Revenue and profit
- IT maintenance budgets
- Avoiding and recovering from IT-based business disruptions
- Inconsistencies in IT resources, procedures, and controls
- The hiring and retention of IT skills
- Improving or sustaining regulatory audit results

Although protecting sensitive data is the top pressure impacting IT among all firms, the handling and protection of sensitive information is a more crucial issue among larger enterprises than among small businesses for two reasons:

1. There are more people with access to sensitive data across larger firms.
2. The global nature of business operations among larger organizations requires compliance with more complex regulatory and legal statutes governing the handling of information than among small businesses operating within local regions.
Improving business results and mitigating financial risk

Business and financial risks

Among the firms with the best business results, the capabilities if impaired or compromised that pose the most business risk include:

- The protection of sensitive information
- The integrity and availability of IT resources
- Compliance with regulatory mandates
- The financial statements and structure of the organization (see Figure 14).

![Figure 14. Business risks](source: IT Policy Compliance Group, 2008)

Moreover, with the exception of disruptions to supply chains and distribution channels, 60 percent or more of the leading firms—those with the best business results—rate IT-enabled business capabilities as posing the most risk for the organization should these be impaired or compromised. In contrast, only 30 percent of firms performing at the norm believe that compromises to IT-enabled business capabilities pose the most risk to the organization. Lastly, less than 10 percent of the organizations with the most stagnant business results see impaired IT-enabled business capabilities as posing the most risk to the organization.
**Financial risk from the loss or theft of customer data**

Firms with the least mature IT GRC practices that have experienced the loss or theft of customer data are enduring financial losses equivalent to 8 to 9 percent of revenue for about a six- to twelve-month period. Although this rate may provide a useful guideline for the worst case, it is not predictive for other firms. The expected financial loss for data loss or theft, derived from benchmarks conducted with 1,461 organizations and confirmed from publicly available data, provides a more predictive set of guidelines for the likely financial loss that will occur, based on the maturity of an organization’s IT GRC practices (see Figure 15).

![Graph showing expected financial loss from theft or loss of customer data](image)

**Capital at risk**

<table>
<thead>
<tr>
<th>Annual revenue</th>
<th>$10 million</th>
<th>$100 million</th>
<th>$1 billion</th>
<th>$10 billion</th>
<th>$100 billion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Least mature</td>
<td>$840,000</td>
<td>$9.6 million</td>
<td>$96 million</td>
<td>$960 million</td>
<td>$7.2 billion</td>
</tr>
<tr>
<td>Most mature</td>
<td>$35,000</td>
<td>$400,000</td>
<td>$4 million</td>
<td>$40 million</td>
<td>$300 million</td>
</tr>
</tbody>
</table>

**Figure 15. Expected financial loss from theft or loss of customer data**

*Source: IT Policy Compliance Group, 2008*
Not all firms are experiencing identical losses after customer data is lost or stolen. For example, some firms are experiencing significant declines in market capitalization accompanied by significant costs without experiencing customer defections and revenue declines. Others have experienced larger declines in customers and revenue, slight declines in market capitalization, and modest increases in costs associated with litigation and cleanup efforts.

The expected financial losses by maturity account for all contributions, including lost revenue from customer defections; lost market capitalization from declines in publicly traded shares; and direct costs for handling subsequent litigation, penalties, settlements, cleanup, data restoration, and customer notifications. Not included are direct costs for improving IT GRC practices subsequent to the loss event.

Despite a specific type of loss, the benchmarks reveal a consistent pattern of expected loss that is confirmed by available data, and that shows a direct relationship between the size of the loss as a percentage of revenue, and the maturity of an organization’s IT GRC program.

The lowest loss rates being experienced by the most mature firms are consistently below one percent of revenue, while the highest loss rates consistently hover between eight and nine percent of revenue among the firms with the least mature IT GRC programs. The vast majority of firms are experiencing financial losses between these two extremes: from nine percent to less than one percent of revenue. Obviously, this is a large loss range, and the losses can be reduced by improving the maturity of IT GRC practices and capabilities.

**Experience of a large retailer**

A large retailer that experienced a theft of customer data in 2007 took $270 million in charges against profits for expenses related to the loss and theft of customer data. The capital loss from the firm’s share-price decline amounted to more than $950 million in the first three months after the event. This decline was slightly reversed to a $680 million loss after the first year.

Recent gains have erased much of the $680 million loss, but there is almost $260 million in value not recovered fifteen months after the loss event occurred. Combined, the loss has been a little more than $530 million, a lot of angst among investors, some among customers, and new expenditures for protecting customer data.

The loss expectancy chart shows that this firm should have expected a loss of nearly $600 million, given its IT GRC maturity levels. Although slightly higher than actual experience, additional costs not publicly reported are not included, nor is subsequent spending to improve IT GRC practices included.
Experience of a large financial services firm

A large financial services firm experienced a theft or loss of customer data in 2006 and took a charge against earnings of slightly more than $100 million. The capital loss predicted by the loss chart for this firm is slightly more than $100 million, indicating closer alignment with actual experience.

This firm is continuing to spend additional monies to improve its IT GRC capabilities and practices. These costs are likewise not included as part of the actual costs incurred for the loss event.

Financial risk from business disruptions due to IT service disruptions

The financial capital at risk from business disruptions that are due to IT systems, applications, and networks being impaired or compromised ranges from 9 percent of revenue to less than 1 percent of revenue.

Unlike the loss or theft of customer data, the financial impact from IT-based business disruptions depends on the number and duration of the disruptions, and how much of the productive capacity of the organization is impaired by such events.

For example, if 100 percent of the productive capacity of the organization is impacted by these disruptions, then the loss rates are going to approach the highest levels. Conversely, if these disruptions impact less than 10 percent of the productive capacity of the firm, then the loss rates are going to be much lower.

The benchmarks consistently show direct relationships between the number of IT service disruption events impacting business operations annually, the number of hours it takes for firms to recover from these disruptions, and the maturity of the organizations’ IT GRC practices.

The factors determining the financial impact from business disruptions due to IT service disruptions include the extent of the impact (less than 100 percent of operations) and the maturity of the organizations’ IT GRC practices (see Figure 16).
For example, the productive capacity within the automotive, leasing, rental, banking, financial services, and manufacturing industries impacted by Internet security threats can result in severe financial consequences for these organizations.

Even in other industries where telecommunications and IT networks are vital, such as retail, entertainment, energy distribution, transportation, hospitality services, government, and law enforcement, among others, IT-led business disruptions can have financial consequences that range from minor inconveniences to dramatic impact on revenue, costs, customers, and reputations.

**Figure 16: Capital at risk from IT-related business disruptions**

*Source: IT Policy Compliance Group, 2008*
Experience of an automotive manufacturer

In 2004, a large automotive manufacturer found that one of its assembly plants was shuttered after an Internet worm infected robotic equipment on its assembly lines. Taking more than a week to clean up and restore operations and return the assembly lines to productive capacity meant that supply chain operations were halted in their tracks. Also impacted were logistics, procurement, transportation, and distribution to dealers. The manufacturer took steps to avoid loss event from occurring again, including isolating the manufacturing sites from other networks, instituting a massive employee education and training program, and implementing continuous monitoring and measurements.

Experience of a rental and leasing company

In 2005, the retail outlets of a leasing company were hit by an Internet security threat. Unable to conduct business for two days in one of the busiest metropolitan areas in the world, this firm asked its customers to do business with competitors and provided the affected customers with compensation to avoid a permanent loss of these customers.

IT GRC: IT governance, risk, and compliance management

The benchmarks show a direct connection between business results, financial risk, and IT GRC indicators for firms, with results clearly aligned based on GRC maturity (see Figure 17).

<table>
<thead>
<tr>
<th>IT GRC Maturity</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Population</td>
<td>20%</td>
<td>68%</td>
<td>12%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer satisfaction</td>
<td>-8.7%</td>
<td>-4.4%</td>
<td>0%</td>
<td>4.4%</td>
<td>8.7%</td>
</tr>
<tr>
<td>Customer retention</td>
<td>-6.3%</td>
<td>-3.2%</td>
<td>0%</td>
<td>3.2%</td>
<td>7.3%</td>
</tr>
<tr>
<td>Revenue</td>
<td>-8.5%</td>
<td>-4.3%</td>
<td>0%</td>
<td>4.3%</td>
<td>8.5%</td>
</tr>
<tr>
<td>Expenses</td>
<td>-6.4%</td>
<td>-3.2%</td>
<td>0%</td>
<td>3.2%</td>
<td>6.4%</td>
</tr>
<tr>
<td>Profits</td>
<td>-6.9%</td>
<td>-3.5%</td>
<td>0%</td>
<td>3.5%</td>
<td>6.9%</td>
</tr>
<tr>
<td>Financial risk from customer data loss/theft</td>
<td>9.6% of revenue</td>
<td>8% of revenue</td>
<td>6.4% of revenue</td>
<td>3.2% of revenue</td>
<td>0.4% of revenue</td>
</tr>
<tr>
<td>Financial risk from disrupted business operations</td>
<td>10% of revenue</td>
<td>3% of revenue</td>
<td>1% of revenue</td>
<td>0.4% of revenue</td>
<td>0.2% of revenue</td>
</tr>
<tr>
<td>Spending on regulatory compliance</td>
<td>37% lower than maximum</td>
<td>3% lower than maximum</td>
<td>3% lower than maximum</td>
<td>20% lower than maximum</td>
<td>52% lower than maximum</td>
</tr>
</tbody>
</table>

Figure 17. Business results and IT GRC maturity

Source: IT Policy Compliance Group, 2008
The questions of whether better compliance practices lead to better data protection, or whether better IT assurance practices lead to more resilient systems that support business procedures, are moot. The evidence from the benchmarks shows an almost one-to-one relationship between actions and practices implemented by an organization to improve GRC maturity with better business results and lower business risk.

The benchmarks also show the opposite: When not implemented, the practices and capabilities are directly linked to worse business results, much higher levels of financial and business risk, and higher spending on regulatory compliance.

Assessing the current state of IT GRC maturity is but a start toward improving the results, business outcomes, and financial risks that are shown to be almost completely aligned with IT GRC maturity.

Once assessed, the next step on the journey to better business results, lower financial risk, and reduced spending on regulatory compliance is to identify the practices and capabilities that are shown to be directly related to improving results.

**Organizational competencies and IT GRC maturity**

There are common organizational practices and capabilities being implemented by the firms with the most mature IT GRC profiles. Possessing better business track records, less financial and business risk, less worry about customer data, lower spending on regulatory compliance, and almost uninterrupted IT services, the actions and capabilities implemented by these firms are an excellent gauge for assessing what is working.

Although there are more details behind these competencies, there is no doubt that if implemented, these competencies can improve results for the 88 percent of firms with less mature IT GRC profiles and worse results than the most mature organizations.

**Who should be involved in IT governance**

The governance of IT is a management function. Focused on delivering greater value from IT services that anticipate and meet the needs of evolving business conditions, it is sometimes a tightrope walk involving a wide range of factors, including resource constraints, objectives, unceasing demand for new or changed capabilities from the business leaders of the organization, quality levels, functionality, and timeliness.

Like any other function in the organization, the governance of IT also involves an understanding of and the management of business risks from the use of IT. As the benchmark evidence clearly shows, business results, financial risks, regulatory compliance results, and spending are all intimately linked with the IT GRC maturity profiles of organizations.
Based on the evidence, from least mature to most mature, the top three organizational functions that make the most difference to improving IT GRC maturity are the involvement of:

1. Senior management
2. Managers and directors in IT
3. The audit committee

Following closely behind these is involvement by:

1. The IT governance committee
2. Staff in IT (including contractors and service providers)
3. Internal and external audit functions
4. Business unit managers (see Figure 18).

![Figure 18. Who's involved in IT governance](image)

*Source: IT Policy Compliance Group, 2008*

These are the top eight functions involved in governing IT. As the findings clearly show, the governance of IT is not the responsibility of a single function or group within the organization. Rather, IT GRC maturity improvements depend on a transparent, shared responsibility: one that is able to successfully meet the very different needs and functions of the organization.
Who should be involved in assessing and demonstrating compliance

Unlike the management and governance of IT, assessing and demonstrating compliance is the act of gathering and demonstrating evidence that the organization’s policies are being implemented, that the controls needed to demonstrate compliance with policy are working and effective, and that the risks the organization faces are understood and being managed. The assessment and demonstration of compliance is often a shared responsibility between audit, IT assurance, internal controls, and IT operations, and most often with the direction of assistance of the IT risk management and IT audit functions.

In addition, the benchmark results show that the legal function plays a critical role in the success of the most mature IT GRC organizations. Whether it is compliance with company policies and legal statutes, responding to requests or summonses for information, or managing regulatory audits, the functions involved in demonstrating compliance among firms with the most mature IT GRC results are dominated by:

- The IT and IT security functions
- The legal function for organizations

After these two, the other functions involved in assessing and demonstrating compliance include finance and internal audit and to a lesser extent the IT governance committee, the audit committee, and compliance and risk management functions in organizations (see Figure 19).

![Figure 19. Who's involved in assessing and demonstrating compliance](source: IT Policy Compliance Group, 2008)
Based on interviews conducted with members, better results for IT GRC are being achieved by firms with an almost activist IT audit function: one where there is a great deal of cooperation between the business units, the entities being audited, the IT assurance function, legal counsel, IT assurance, and operations. Conversely, organizations with passive IT audit functions and IT audit functions not auditing technical controls are among the organizations with lower IT GRC maturity profiles, worse business results, heightened business risks, and worse regulatory compliance results.

**Employee training: A culture of compliance**

The benchmarks show that a culture of compliance, reinforced by senior management and implemented with formalized training for employees, is one of the core competencies being implemented by organizations with the most mature IT GRC profiles.

The most mature firms are implementing and delivering on-demand training for employees, more consistently, when compared to all other organizations. Most often taking the format of Web-based education, training, the top subjects for employee training among the most mature organizations include ethics and codes of conduct, IT compliance, IT security and data protection policies, regulatory policies and procedures, discrimination and harassment, and emergency response and restoration procedures (see Figure 20).

Figure 20. Employee training and IT GRC maturity  
*Source: IT Policy Compliance Group, 2008*
Organizational actions to improve IT GRC results

Actions speak louder than words, especially when the actions are aligned with better business and financial results. For example, the primary actions taken by the most mature IT GRC firms include:

- Improving IT risk, assurance, and data protection practices
- Improving IT audit, risk, and compliance practices
- Adjusting the focus of and spending within IT to support these

After these three, the actions most closely linked with improved IT GRC maturity include acquiring IT capabilities to improve results, improving project and portfolio management practices, improving IT skills and retention programs, codifying IT service levels and contracts, and improving IT governance practices. Nearly all of the actions taken by firms are aligned with IT GRC maturity improvements, as well as top-line and bottom-line business results (see Figure 21).

The interesting anomaly, improving IT governance practices, indicates that specific actions, practices, and capabilities being taken by the least mature firms are not resulting in improvements; rather, the actions being taken by the least mature firms are actually retarding results, are counterproductive, or are insufficient when compared with the results being achieved by the most mature firms.

Figure 21. Organizational actions to improve IT GRC results

Source: IT Policy Compliance Group, 2008
As such, the actions and specific practices and capabilities being employed by the most mature IT GRC firms provide the best gauge for ascertaining the practices and capabilities needed by a majority of organizations, 88 percent of which are having worse business results and higher financial loss experiences than the most mature firms.

Business risks, assessments, and priorities
Given the predictable downside financial risk from the theft or loss of sensitive data and the loss of productive capacity from IT service disruptions, every firm should evaluate whether it should ignore the risks, transfer the risks, or mitigate the risks. Ignoring IT-based risk is impossible unless the organization wants to turn off all the IT systems that assist and enable business procedures. Transferring a portion of the financial risks may be possible. Mitigating these risks is almost a necessity to avoid reputation and brand damage, in addition to the financial consequences of these risks.

Assessing the risks
In addition to the magnitude of financial loss occurring after the loss or theft of customer data or from business disruptions, the frequency of occurrence of loss events must be taken into account when prioritizing risk. Organizations with the most mature IT GRC programs are delaying the onset of financial loss from the theft or loss of customer data, and from business disruptions due to IT service disruptions (see Figure 22).

Figure 22. Likelihood of primary IT GRC risks
Source: IT Policy Compliance Group, 2008
Unless an organization wants to start over, data loss or theft and their attendant harm to reputations and brands is a risk that calls for mitigation. However, not all IT service-level disruptions have equal downside risk for the organization. As a result, it is important to identify and isolate disruptions from IT services that will most impact the organization, making sure to account for embedded and unseen dependent business procedures that may not be apparent at first.

**IT GRC functions and practices**

The key IT governance competencies and practices being implemented by the most mature IT GRC organizations include:

- Strategic IT planning and business alignment
- IT performance assessment and measurement
- IT security, assurance, and risk management
- IT audit and compliance management
- IT operations and resource management

These are the five primary IT GRC activities currently implemented by a majority of the firms with the best business results and the least financial risk (see Figure 23).

*Figure 23. IT GRC functions and practices*

*Source: IT Policy Compliance Group, 2008*
How do you know whether the value being delivered by IT meets expectations, or that that use of IT resources is not placing the firm at greater risk? The only way to discern the answers to these questions is to measure results. In addition to the five primary IT GRC functions, the most mature firms also routinely assess and report on the status of IT governance on a much more frequent basis than all other firms. On average, the assessment of these functions by the most mature firms takes place once every five to six weeks.

By contrast, the least mature firms are not routinely assessing the status of these key functions. Instead of once every five to six weeks, the average rate of measurement among the least mature organizations is once every six months.

Lastly, the majority of the firms operating at the norm are conducting these assessments nearly once every quarter (see Figure 24).

More frequent assessment and reporting on the status of these functions for IT governance is leading to better delivery of business value and lower financial risk among the most mature organizations.

**Framework usage and IT GRC maturity**

Frameworks are evolving sets of practices that are shown to work, and represent codified bodies of knowledge based on past experience. However, not all frameworks are created equal: Some focus on procedures and processes, others focus on quality, others focus on the management of resources to achieve business objectives, others on detailed best practices within IT, and still others focus on technical software and hardware controls.
**Which works: Components of many, or selection to drive results?**

Despite being widely available, there is a significant difference in the way firms are employing frameworks that is directly related to the maturity of IT GRC. Most firms—the 88 percent not operating at the most mature levels—are employing a buffet-style approach to the use of frameworks. The majority of firms are electing to choose components from multiple frameworks. For instance, the majority of the least mature firms are choosing to select components from four to five frameworks for use within IT operations, IT assurance, and IT audit. In contrast, less than 20 percent of these same firms are selecting even one framework for the governance of IT value being delivered by the firm. Among normative IT GRC firms, the same buffet-style behavior occurs, but the number of frameworks dwindles from four or five to two or three. Finally, by the time some of these firms emerge among the most mature, the number of frameworks increases to four or five again, but a selective weeding out of frameworks has occurred. The buffet-style selection behavior has been replaced by a decided focus on the primary frameworks that are being relied upon to assist the organization with its own framework for its objectives against which results are measured (see Figure 25).

---

**Figure 25. Frameworks, least to most mature**

*Source: IT Policy Compliance Group, 2008*
**Frameworks for managing the value delivered by IT**

The primary frameworks being employed by the most mature organizations for managing and governing the value delivered by IT include:

- Six Sigma, or a Continuous Quality Improvement program
- Project management maturity or IT portfolio management
- A capability maturity model and a balanced scorecard

**Frameworks for IT operations, assurance, audit, and vendor management**

The primary frameworks being employed by the most mature organizations for managing agility, risk, and compliance within IT operations to meet organizational objectives and policies include:

- ISO, CobIT, and related IT process frameworks
- The CIS benchmarks covering configuration best practices for technology controls
- SDLC for managing projects and change

**Measurable results, Continuous Quality Improvement, and IT GRC**

A Continuous Quality Improvement cycle for Six Sigma and Deming cycles is being implemented for IT governance and within IT operations, IT assurance, and IT audit by the majority of the most mature firms (see Figure 26).

---

**Deming cycle: PDCA**

- **Plan:** Establish objectives and procedures to deliver results per specifications.
- **Do:** Implement the procedures.
- **Check:** Monitor the procedures against objectives and specifications.
- **Act:** Apply actions to improve results. Further modify procedures as appropriate.

---

**Six Sigma: DMAIC**

- **Define:** Plans that must be in place to improve results.
- **Measure:** The systems that support the plans.
- **Analyze:** Gaps and develop “desired state.”
- **Improve:** System elements to improve results.
- **Control and maintain:** To sustain results.

---

**Figure 26. Continuous Quality Improvement and IT GRC**
*Source: IT Policy Compliance Group, 2008*
Improving business results and mitigating financial risk

Using a Continuous Quality Improvement program is essential to increasing the maturity of IT GRC, with the value being delivered by better business results, the management of risk, and compliance with internal and external policies and statutes. Although Six Sigma is identified as the primary Continuous Quality Improvement framework for management, the research also shows that full-bore Six Sigma within IT operations is resulting in less than optimum results. For this reason, simpler and less hidebound approaches to continuous quality improvement in IT operations involving a cycle of assessment, improvement, measurement, and repetition is appropriate for most organizations.

In addition to specific practices and capabilities, it is continuous quality improvement, integrated from IT operations through the balanced scorecard, that is responsible for driving solid improvements in IT GRC maturity, lower financial risk, and better business results among the most mature firms. Whether it is data protection, regulatory compliance, or the delivery of value from IT, the most mature firms are continuously improving quality in an integrated and repeatable manner, with practices and capabilities being implemented to support results (see Figure 27).

**Insight**
In addition to specific practices and capabilities, it is continuous quality improvement, integrated from IT operations through the balanced scorecard, that is responsible for driving improvements.

---

**Figure 27. IT GRC among the most mature firms**

*Source: IT Policy Compliance Group, 2008*
Through the balanced scorecard, the most mature firms are balancing risk and reward, establishing policies and control objectives, and continually assessing the risk/reward balance to ensure it is appropriate. Balancing projects, resources, and timeframes is accompanied by more detailed procedural and process frameworks and control statements related to procedures that are implemented in IT. These are accompanied by policies and procedures (manual and technical) for controls implemented in IT that reflect the risk/reward balance being sought by the organization.

Whether the objective is increased revenues and profits, lower financial and reputation risks, or greater systems resiliency for business purposes, the most mature organizations are constantly seeking to improve results. Although not perfect, the most mature organizations are continuously assessing the risk/reward balance, determining what improvements or changes need to be introduced, measuring the results, repeating these steps, and implementing specific practices and capabilities to achieve their objectives.

**Practices and capabilities aligned with IT GRC maturity**

Putting IT GRC into action involves repeatable practices and procedures. There are ten key practices and capabilities being implemented by the most mature firms.

**Actions taken in IT to improve IT GRC maturity**

The actions taken in IT to improve IT GRC results include:

- Improving IT controls and procedures
- Protecting data on PCs and laptops
- Segmenting and limiting access to sensitive data
- Increasing the frequency of monitoring and measurements (see Figure 28)

The additional actions taken by the most mature firms include:

- Delivering training for employees
- Identifying the leakage of sensitive data
- Correcting gaps in controls and procedures
- Automating the collection of IT audit data

<table>
<thead>
<tr>
<th>Practices and capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Access to sensitive and protected data on PCs and laptops is segmented and protected.</td>
</tr>
<tr>
<td>• Meaningful and measurable control objectives and policies based on business risks are employed.</td>
</tr>
<tr>
<td>• IT policies, process frameworks, and control objectives are mapped to one another.</td>
</tr>
<tr>
<td>• Common IT procedures are employed for audit.</td>
</tr>
<tr>
<td>• Three times more controls are employed than objectives.</td>
</tr>
<tr>
<td>• Consistent configurations and common IT procedures are employed.</td>
</tr>
<tr>
<td>• Automation is widely employed.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>• Policy-in and audit-out for technical controls is managed.</td>
</tr>
<tr>
<td>• IT change control and unauthorized change prevention are implemented.</td>
</tr>
<tr>
<td>• Monitoring, measurement, and reporting occur, from continuously to once a month.</td>
</tr>
</tbody>
</table>
Clearly, the most mature firms are enjoying better results because these organizations are taking fundamental actions and implementing practices in IT that are very different from all other firms.

*Segmenting and limiting access to sensitive data*

The most common tactic employed by firms that must pass the PCI DSS audit (relevant to firms processing and holding credit card data) is to isolate the systems that hold, process, and touch credit card data covered by the PCI audit requirements. The number of systems subject to the PCI audit can be reduced significantly by segmenting and limiting access to the data. By segmenting access to the systems that are used to process credit card data, firms are significantly reducing the impact and costs of conforming with PCI DSS audits.

Accomplished in a variety of ways, including network isolation, software isolation, hardware isolation, firewalls, controls on physical access, and controls on authorized access, the segmentation and limits imposed on access reduces the number of systems that must be audited to pass the PCI audit.

![Figure 28. Actions taken in IT to improve IT GRC results](image)

*Source: IT Policy Compliance Group, 2008*
For many successful firms, passing PCI audits also involves isolating the systems, networks and applications that touch sensitive data, resulting in reductions to the number of systems that must be audited by a factor of 10. For example, firms with 4,000 systems typically find that fewer than 400 of these actually have anything to do with the PCI audit.

Different strokes for different folks

Not all firms have to pass the strict requirements of PCI audits. Some organizations may have more pressing issues to confront and others less. For example, the law enforcement, utility generation, transportation, and chemical and pharmaceutical manufacturing sectors have very different pressures and different regulatory audit mandates than do manufacturers, legal service firms, banks, retailers, insurance companies, and financial service firms. As an extreme example, some organizations have placed lead shields around buildings, and are employing cryptography for everything transmitted outside the buildings. Although this approach is not common, there are multiple ways of segmenting and limiting access to sensitive data. Whichever approaches to controlling the segmentation and limitation of access to sensitive data are employed, this key action is being taken by firms with the most mature IT GRC profiles and practices.

Frequency of reporting for IT procedures and functions

The most mature firms are reporting on the effectiveness of IT procedures on a more frequent basis, on average once every four to six weeks (see Figure 29).

![Figure 29. Frequency of reporting on IT procedures, activities, and controls](source: IT Policy Compliance Group, 2008)
The most frequently reported areas include the status of information protection controls; physical security; incident response; business continuity and disaster recovery; IT access controls, including those for applications, databases, networks, and other systems; personnel security; and IT assets, configurations, and settings.

Unlike the most mature firms, the frequency of reporting among 88 percent of all organizations is taking place, at best, once every six months. This finding is in line with organizations that do not have a Continuous Quality Improvement program in place. Infrequent reporting by a majority of firms means that any measurements being taken are too infrequent to effectively improve results.

**Frameworks for IT assurance, audit, and IT operations**

The frameworks employed within IT for assurance, information security, and regulatory compliance that are making the most difference among the most mature firms include:

- ISO 17799 and 27000
- ITIL
- CIS benchmarks
- SDLC
- CobiT

The research shows that the most mature IT GRC firms are consistently employing these five frameworks within IT operations, assurance, and audit. The ISO and CobiT frameworks are more similar to each other than to others, each being a process view of IT activities. Some firms select one or the other, while others select both: CobiT for financial audit and ISO for IT activities. Among the most mature firms, mapping the activity controls from one to another, along with sufficient documentary evidence, is assisting in the effort to more smoothly pass audit.

The ITIL framework is all about service levels: a requirement for measuring the level of service delivered internally and by third-party service vendors, including offshored and outsourced IT services. The CIS benchmarks are best practices at the machine and systems levels for IT assurance. These benchmarks are technology specific. Where the CIS benchmarks are machine focused, the ISO and CobiT frameworks are functional and practice focused.

**Necessary and sufficient**

IT service level agreements are very useful for describing service levels for IT, and CobiT is the standard lingua franca employed by external auditors conducting Sarbanes-Oxley (SOX) audits. However, organizations are very unlikely to fail a SOX audit for deficiencies in IT general controls, or for that matter for deficiencies in ISO-based controls that are mapped to CobiT. However, without the CIS benchmarks, the research shows a higher predisposition to more business downtime and greater risk from the loss or theft of sensitive data, including customer data. CobiT, ITIL, and ISO may be necessary, but the CIS benchmarks are sufficient for improving IT GRC results.

**Insight**

CobiT, ITIL, and ISO may be necessary, but the CIS benchmarks are sufficient for improving IT GRC results.
**Control objectives and controls**

The most mature firms have more controls than control objectives, while the least mature organizations have more objectives than controls (see Figure 30).

![Figure 30. Control objectives and controls](image)

**What's a control objective?**

Control objectives are policies describing the risks. For example, a control objective might start with: “We will safeguard and not lose or have stolen any customer data.” In addition to being objective statements about risk, control statements also include the policies implemented by the organization, the procedures and controls being implemented to mitigate the risks, the objectives for what constitutes acceptable performance results, Continuous Quality Improvement objectives, and key performance indicators being measured. Together, these elements constitute effective control objectives for IT GRC being implements by the most mature organizations.

**Control objectives and IT GRC related business risk**

Control objectives for IT GRC commonly address business risk, financial risk, legal risk, regulatory risk, reputation risk, and IT-related risks. Although unusual, control objectives for IT GRC could also address market risk, currency risk, legal risk, labor risk, supply-chain risk, and distribution channel risk, among others.

The business risks are shown to include financial loss from the loss or theft of customer data and business disruptions that result from IT service disruptions. Legal risks include the loss of customer data and legal summonses and requests for the production of email, records, and other data among other risks.
Control objectives for IT GRC encompass regulatory risk as these relate to civil penalties, criminal penalties, fines, and reputation risk, and might be related to J-SOX, European Data Privacy Directives, specific industry requirements, or any number of other regulatory mandates and audits. In addition to these, there are also risks associated with the use of different IT service delivery options and technologies. For example, outsourcing the ERP systems or sales automation systems poses very different risks than implementing and sustaining these internally. Similarly, a firm conducting acquisitions is going to have different risks associated with the merger of different IT systems, procedures, and people than firms not conducting acquisitions. The use of technology is also associated with different risks. For example, file sharing and instant messaging services pose unique business risks that do not exist with mainframe transaction systems and the use of common proxy authentication services for reservation systems.

**Key performance indicators and control objectives**

Key performance indicators are a subset of what should be included in control objectives. Such indicators include:

- Metrics that can be measured
- Metrics that provide trend indications about the risk profile of the organization

The benchmark results show that the key performance indicators are clearly focused on IT general controls and IT assurance in particular.

**One size does not fit all**

In addition to key performance indicators, the benchmarks show the ratio of controls to control objectives is directly related to making continuous quality improvements to IT GRC maturity.

The reason the ratio of controls to control objectives is important is that not all firms are operating with a control objective count as low as 30. In fact, the research shows that the number of control objectives is currently related to firm size, with small businesses having about 25, midsize organizations having about 50, and large enterprises having 75 or more control objectives, on average.

For a large enterprise with 75 control objectives, the research shows the optimum number of controls would be 225 or more. A continuous quality improvement for this firm might be to reduce the number of objectives over time, thereby reducing the number of controls. If this firm had only 125 controls, the improvement program might be to simultaneously reduce the number of control objectives while increasing the number of controls.
The ratio of controls to control objectives provides a size-independent method by which to ascertain the improvements in these two that are most appropriate for any organization. Remember, a larger set of control objectives with a correspondingly larger set of controls is going to be more costly to sustain than a smaller set of objectives and controls (see Figure 31).

Figure 31. Ratio of controls to control objectives
Source: IT Policy Compliance Group, 2008

What’s a control?
Controls are the procedures put in place to mitigate risk. These could be procedural or manual in nature, or could be implemented in technology. For example, a control might ensure that changes to underlying datasets or applications can only be performed after the approval of someone other than a database administrator.

Similarly, access to sensitive information may be controlled by a technical access control, including user accounts and entitlements, directories, application logon systems, server logon systems, network access controls, and cryptographic controls on information content. The list of all possible controls is beyond the scope of this research report.

However, the research shows the firms with the least mature IT GRC results are implementing a majority of controls as procedural or manual controls. In contrast, the organizations with the most mature IT GRC results have reduced the proportion of manual or procedural controls to 50 percent or less, while increasing the proportion of technical controls to 50 percent or more. Among firms with the most mature IT GRC profiles, automated technology controls have slightly edged out manual procedural controls to mitigate risk while delivering better business results (see Figure 32).
Improving business results and mitigating financial risk

![Graph showing the ratio of controls to control objectives]

**Figure 32. Procedural and technical controls**

*Source: IT Policy Compliance Group, 2008*

**Automation of technical controls**

In addition to a 50 percent mix of procedural and technical controls, the most mature IT GRC firms have also automated a majority of the technology controls, with almost 100 percent of the available technical controls being automated.

This contrasts sharply with most firms operating at the norm that have automated less than 30 percent of a smaller set of technical controls, and even more sharply with the least mature firms, who have fewer technical controls with less than 10 percent of these being automated.

Ranging from 70 percent to close to 100 percent, the most mature firms have taken two approaches that have clearly contributed to improved results, as follows:

1. More technical controls have been deployed to act as proxies for procedural controls.
2. Almost all of the technical controls have been automated.

In contrast, the majority of firms are automating less than 50 percent of the available controls for IT GRC, and the least mature are automating 10 percent or less of the available controls for IT GRC (see Figure 33).

**Insight**

Continuous quality improvement dictates moving from manual controls to a profile that is evenly mixed between manual and automated technology controls...
Improving business results and mitigating financial risk

Figure 33. Automation of technical controls
Source: IT Policy Compliance Group, 2008

Connect the dots: Technical controls, policies, and control objectives

Control objectives operate on technical control mechanisms by way of policy. From high-level policy that is related to organizational objectives, legal statutes, and regulatory requirements, control objectives must then be translated to IT assurance descriptions and then to binary mechanisms implemented within technical controls.

Unfortunately, there are often gaps between human-readable policies and the implementation of policy in technical control mechanisms. Although there is a great deal of assistance to automate this mapping, less than 30 percent of all firms are currently taking advantage of this automation.

Whether accomplished by hand or mapped using software, the input for any control activity or action is fundamentally policy, which the technical mechanisms use to make decisions, and the output of the action, which only consists of audit logs containing evidence about conformance to policy.

This is one of the key reasons why the most mature organizations are consistently measuring, monitoring, assessing, and reporting on control effectiveness: the devil is in the details of the log files (see Figure 34).
The analog to consistent measurement of log files for manual procedural controls is found from more consistent self-assessment of manual procedural controls conducted among the most mature IT GRC firms. The Continuous Quality Improvement objectives for the firms not operating at the most mature level of IT GRC include rationalizing:

- Policies across control objectives
- Controls and control objectives for the frameworks being employed for internal and external audit
- Self assessment of manual procedural controls
- Consistent measurement of technical controls

Among the most mature firms, these efforts are leading to rational control objectives, policies that are based on relevant IT GRC risks, more controls per objective, all of which are accompanied by much clearer and transparent communication and evidence for internal and external audit.
Automating activities in IT

The most common activities in IT that are being automated by the most mature IT GRC firms include:

- Ongoing monitoring and measurements
- Collection of audit-related data
- Procedures and controls

Further ahead than the general population, the activities automated by the most mature firms also include ongoing assessment of compliance with policy, remediation, and change management (see Figure 35).

By comparison, very few of the least mature firms automate procedures and controls and only marginally more of these firms are automating other activities. The two activities most automated among the least mature include ongoing monitoring and reporting, and the collection of IT audit data. However, given fewer controls than control objectives among the least mature, and the scant number of technical controls being automated by these firms, the extent of automation of IT GRC activities is low, at best. In comparison, the majority of firms operating at the norm are somewhat in the middle when it comes to automating these IT GRC activities.
Frequency of controls assessment, measurement, monitoring, and reporting

The most mature firms assess and report on the effectiveness of controls much more frequently than all other firms. In fact, on average, these firms are measuring and reporting 22 times per year. The minimum frequency for controls effectiveness reporting among the most mature is once every month—a finding from the benchmarks that has not changed across more than 2,600 organizations (see Figure 36).

In contrast, the least mature firms are measuring and reporting on the effectiveness of controls once to twice per year, while the majority of firms operating at the norm are assessing and reporting on the effectiveness of controls once per quarter, on average.

![Figure 36. Frequency of control assessment and reporting](source: IT Policy Compliance Group, 2008)

The infrequency with which a majority of organizations are assessing the effectiveness of controls is similar to saying that trees in the forest cannot fall if we are not there to hear or see them fall. But trees fall, whether we are there or not.

When it comes to IT GRC, business results, risks, financial losses, reputation risk, and business uptime all depend on continuous assessment and measurement; not measuring the effectiveness of controls is very risky for the business.
Assessment, measurement, and monitoring of IT general controls

What are the most mature firms measuring more frequently? The answer is: Almost all major IT systems, including IT systems; operating systems; applications; databases; network equipment and software; IT system log files and controls; and user accounts entitlements, permissions, administrative groups, and privileged access accounts. Nearly 60 percent or more of these firms are routinely measuring all of these IT systems once per month or more (see Figure 37).

Although not as widely practiced, the measurement of applications, the Web, email, Internet systems, Internet threat controls, and file-level permissions are also being assessed more frequently by the most mature firms.

If a loss or theft of customer data occurs and no one notices, did it really ever happen? If operating at the least mature GRC levels, it may take months or years to find out, and several incidents and financial harm to change behavior—hopefully it will not be too late.
What color is the IT change management program?

Change management is to IT what quality control is to manufacturing. Change management is responsible for ensuring that changes in IT do not impact business information, business procedures, customer satisfaction, customer retention, revenue, expenses, and profit. And when it comes to IT assurance, change management is one of the bedrock practices for assuring the reliability of service levels, and the integrity and confidentiality of information.

The most mature firms are almost always implementing a full IT change management program that tracks change requests from inception to retirement, and every step in between (see Figure 38).

![Figure 38. Completeness of IT change management programs](source: IT Policy Compliance Group, 2008)

In contrast, normative firms are only sometimes implementing aspects of a full IT change management program and less mature organizations are less assiduous still about IT change management.
A Continuous Quality Improvement objective for a majority of firms should be to fully implement an IT change management program, from inception, assessment, and testing to completion. A negative side effect of the widespread culture of convenience with which most IT is now associated, due in large part to designed-in simplicity, is that formal IT change management practices are slowly becoming a lost art.

If current staff in IT have little or no experience with change management, it may be necessary to either hire consultants with experience to assist in developing and implementing appropriate IT change management practices, or hiring staff to develop and sustain a change management program that is fit for the company’s purpose.

In either event, a complete IT change management program is one of the hallmark practices that the most mature organizations implement. In addition, these firms also use a strategy of prevention, when unfettered control could lead to unacceptable risks.

Preventing unauthorized change

In addition to implementing quality control in IT in the form of a complete IT change management program, the most mature firms are also preventing unauthorized change to IT resources on production systems (see Figure 39).

Implementing an almost real-time notification for critical changes to IT systems that violate policy, the most mature firms are preventing unauthorized change and the introduction of unauthorized IT systems, software, and network components to major IT resources, including unauthorized change to the following: network systems and software; Web, email, and Internet systems; registries and directories; databases; servers and operating systems; and user accounts, entitlements, and permissions. Close behind these major systems are changes to Internet threat controls, application software, IT security log files and controls, administrative groups, and system privileges.

Figure 39. Preventing unauthorized change to IT resources

Source: IT Policy Compliance Group, 2008
Not tested by the benchmarks but confirmed from interviews conducted with members of the Group, many firms are also employing change management when PCs, laptops, and PDAs want to access corporate production networks. If policies are not met, these devices are being prevented from accessing corporate networks until specific policy objectives and authorizations have been met.

The biggest impact of preventing unauthorized change is that the most mature firms are spending much less time on remediation and fixing problems, when compared with the majority of firms. Less than 10 percent of the time being spent on IT GRC activities among the most mature firms is spent on firefighting, remediation, and fixes. In contrast, the least mature firms are spending nearly 60 percent of their time putting out fires and fixing problems.

A Continuous Quality Improvement program for IT GRC depends upon more frequent assessment of controls, a complete change management program, and an unauthorized change prevention management program.

**IT audit strategy and scope**

Current IT audit strategy and the scope of IT audit is not materially impacting results for firms. For example, common IT procedures have been adopted by most organizations, but this has not resulted in a material difference in IT GRC performance results among firms (see Figure 40).

![Bar chart showing IT audit strategy and focus](https://via.placeholder.com/150)

**Figure 40. Audit strategy and focus**

*Source: IT Policy Compliance Group, 2008*
Most organizations are conducting IT audit the old-fashioned way, by auditing different business function and business entities serially and separately. This approach is resulting in auditing the same IT systems and applications multiple times. In addition, IT auditors are conducting separate audits in support of different regulatory audits, as well as conducting separate audits of common IT procedures.

Almost all of IT auditors who were interviewed say that changing the focus and strategy to leverage common IT procedures across business functions will transform current workload and IT GRC maturity profiles into a more smoothly functioning system with fewer surprises, less loss of customer data, and more reliable IT systems and business procedures.

**Putting IT GRC into action**

The evidence is clear. Improving IT GRC is directly related to significant benefits being achieved by the most mature firms, including better business results and lower financial risks. However, benchmarks show that these improvements also come at additional expense.

*More money being spent on IT assurance*

The research shows that proportionally more funds are being spent by the most mature IT GRC firms on the IT assurance and audit functions to improve results (see Figure 41).

<table>
<thead>
<tr>
<th>Better business results</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Higher customer satisfaction</td>
</tr>
<tr>
<td>- Better customer retention</td>
</tr>
<tr>
<td>- Higher revenues</td>
</tr>
<tr>
<td>- Larger profits</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lower financial risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Lower customer data loss or theft</td>
</tr>
<tr>
<td>- Less business downtime</td>
</tr>
<tr>
<td>- Less money spent on regulatory compliance</td>
</tr>
</tbody>
</table>
Although not all organizations have the same size IT budgets, the benchmarks show consistency in the size of IT budgets based on the size of an organization. Moreover, the research findings consistently show that firms operating within the norm, and those operating at the least mature IT GRC levels, are spending less on IT assurance and security, while not implementing the practices and capabilities of the most mature firms.
Spending on regulatory compliance

Annual spending on regulatory compliance depends on the size of the organization, as well as its IT GRC maturity. Total spending on compliance includes fees paid to auditors, consultants, internal audit, IT, legal assistance, and labor costs to comply with legal statutes, external regulations, and audits. Small businesses have fewer audits than the largest of enterprises, and spend proportionally much less on regulatory compliance than larger enterprises. The benchmarks also show that spending on compliance is directly related to the maturity of IT GRC practices (see Figure 42).

For example, average annual spending on regulatory compliance among firms with $1 billion in revenue is $7.6 million when the firm is performing at a normative maturity level of 2.5. However, another $1 billion firm operating at a more mature IT GRC level of 4.5 is spending $4.9 million on regulatory compliance, a difference of $2.7 million annually, or a 35 percent reduction in spending compared with a firm of the same size operating at the lower maturity level.

![Figure 42. Annual spending on regulatory compliance](source: IT Policy Compliance Group, 2008)

The research findings consistently show an increase in spending on regulatory compliance as maturity increases, and a subsequent reduction in spending as firms improve the practices and capabilities that lead to higher IT GRC maturity, improved business results, and reduced business risk. Annual spending on regulatory compliance is consistent by company size and industry, indicating that improved IT GRC maturity is resulting in cost savings for all firms.
Time spent on regulatory compliance by IT assurance and audit

In addition to the total amount spent on regulatory compliance, the benchmarks show a similar pattern to the amount of time, or labor, being allocated to assessing and demonstrating regulatory compliance. Costs for labor increase through the normative stage and then decline as firms improve the practices and capabilities leading to more mature IT GRC results (see Figure 43).

Figure 43. Time spent on regulatory compliance
Source: IT Policy Compliance Group, 2008

Among the common reasons cited by participants at the most mature firms for the decreases in spending on regulatory audit and the time spent on compliance are:

- Consistency between internal policies and industry-focused frameworks being employed by auditors
- Consistency between expectations, employee education, and behavior
- More automation of controls and activities
- Much less time spent on remediation and fixing problems
- Consistency between policy documentation, procedures, and practices for audit review
- Greater transparency of procedures, practices, and evidence for audit review

Although not all organizations will realize the same level of savings (some may achieve more and some less), the benchmarks clearly show that annual spending related to regulatory compliance declines significantly with improvements in the maturity of IT GRC practices and capabilities.
Managing the improvements

Improving IT GRC maturity will come with some additional costs. Depending on where the organization finds itself on the maturity curve, additional costs may include more technical controls, a Continuous Quality Improvement program, employee education and training, and management reporting systems. As part of the exercise to put IT GRC into action, it is important to compare the additional costs against reduced spending and lower financial risks. For many organizations, the financial benefits are going to outweigh the costs by orders of magnitude (see Figure 44).

<table>
<thead>
<tr>
<th>Financial risks</th>
<th>Current state</th>
<th>Desired state</th>
<th>Increase (decrease)</th>
<th>Percentage change annually</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data loss and theft</td>
<td>$56 million every 3 years</td>
<td>$24 million every 10 years</td>
<td>($16.3 million annually)</td>
<td>(87%)</td>
</tr>
<tr>
<td></td>
<td>$2.3 million 49 hours annually</td>
<td>$0.53 million 11 hours annually</td>
<td>($1.77 million 37 hours annually)</td>
<td>(77%)</td>
</tr>
<tr>
<td>Business downtime</td>
<td>$7.6 million annually</td>
<td>$4.9 million annually</td>
<td>($2.7 million annually)</td>
<td>(36%)</td>
</tr>
<tr>
<td></td>
<td>34% annually</td>
<td>21% annually</td>
<td>(13% annually)</td>
<td>(38%)</td>
</tr>
</tbody>
</table>

* For an organization with $1 billion in annual revenue or budget

**Figure 44. Financial impact of IT GRC maturity**

*Source: IT Policy Compliance Group, 2008*

The example chosen is for a firm with $1 billion in annual revenue currently operating at a maturity level of 2.5 that desires to improve the maturity of its practices and capabilities to level 4.5. This firm would see an 87 percent decline in annualized financial capital at risk from the loss of data or theft by improving its IT maturity from norm, at 2.5, to one of the most mature, at 4.5 on the IT GRC maturity scale. The firm would also experience a 77 percent decline in annualized financial risk from business disruptions due to improvements in IT GRC practices and capabilities. Similarly, the firm would experience a 36 percent decline in annual spending for regulatory compliance and a 33 percent decline in annual spending on labor related to assessing and demonstrating compliance for external auditors.
The benchmarks clearly show that improved business results, savings from reduced spending for regulatory audit, and reduced financial risk make it worth the effort to take the next steps.

Assess, improve, measure

Improving IT GRC maturity practices is its own quality improvement procedure that, at its core, simply means assessing the current state of IT GRC maturity, identifying which maturity profile is optimum for the organization based on business and financial results, identifying gaps in current practices, improving practices and capabilities, and measuring the results (see Figure 45).

Some practices and capabilities may be further ahead than what is required to improve results, while other practices and capabilities will be further behind. After improving capabilities and practices, firms should do the following:

- Assess the maturity of the organization.
- Determine the business and financial outcomes from the improvements.
- Identify and implement the next practices and capabilities to improve.
- Measure results and repeat the procedure.
The integrated approach to IT GRC

The research identifies the key organizational competencies being exploited by the most mature firms to drive better results. These include: Greater senior management involvement; involvement by the audit committee; leadership among IT, legal, audit and financial; improvements to IT risk assessments, data protection, IT audit, risk and compliance practices; a Continuous Quality Improvement program that extends from senior managers all the way through operations (see Figure 46).
The research also reveals the practices and capabilities that are most responsible for driving better results, including:

- Protection and segmentation of access to sensitive data
- Measurable control objectives based on reward and risk
- Rationalization of policies and frameworks
- Common IT procedures
- Consistent IT configurations
- More technical controls
- Automation of technical controls and IT assurance and audit activities
- Management of policy and audit for technical controls
- IT change management and the prevention of unauthorized change
- Continuous monitoring, measurement, and reporting

The firms with the best business results and the lowest financial losses and risks are employing an integrated IT GRC program merging the delivery of IT value with the management of risk, legal, and compliance objectives. The approach adopted by the most mature firms starts with the balanced scorecard, employs a Continuous Quality Improvement program throughout IT, and connects the dots between IT operations, IT assurance, IT audit, IT management, and the business results of the organization.

It is obviously going to be easier for a firm currently operating at maturity level 3.5 to move to a maturity level of 4.5 than for a firm currently operating at maturity level 2.5 to do so. Rather than trying to do too much at once—moving from level 2.5 to level 4.5—it may make more sense to take smaller but critical steps on the journey to improving results by improving IT GRC maturity.

A phased approach is more likely to result in increased chances of success, less risk, more measurable value for the organization, higher revenues, improved profits, greater customer satisfaction and retention, less financial risk, and more reliable IT services, all accompanied by less concern, time, and money being spent on regulatory compliance.
## Appendix A: GRC CMM tables

<table>
<thead>
<tr>
<th>IT GRC maturity level</th>
<th>Description</th>
</tr>
</thead>
</table>
| Level 0              | **Nonexistent procedures and practices**  
There is no ongoing oversight of IT related activities to ensure that an enterprise’s IT services add value to the organization and that IT-related risks are appropriately managed.  
                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Level 1              | **Initial/ad hoc procedures and practices**  
IT initiatives are driven by senior managers and primary business stakeholders, based on the changing needs of the business. Problems are resolved on a project basis with teams formed and dissolved as needed. Routine governance activities do not take place. No one realizes that more formalized oversight of IT is required.  
                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Level 2              | **Repeatable but intuitive procedures and practices**  
Governance of IT depends on the experience of IT managers, with limited involvement from business stakeholders. Most IT initiatives are funded based on prior year spending, with little flexibility built in for expected business change. Senior managers become involved in IT when major business initiatives are off-track. IT successes or failures are typically limited to technical measures. Oversight of IT is focused on case-by-case business issues that arise.  
                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Level 3              | **Defined procedures and practices**  
Informal practices are formalized and institutionalized, with relatively simple and unsophisticated measurement and assessment techniques. Specific procedures are developed to govern IT activities. External audit frameworks are utilized to assess the effectiveness of IT in delivering value. The mitigation of risk from IT operations is handled on a case-by-case basis with no consistency.  
                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Level 4              | **Managed and measured procedures and practices**  
Procedural and practice frameworks are defined for oversight and management of IT activities. These frameworks are used as the basis for governance of IT in the organization. Common IT procedures are identified and selected areas for improvement are based on these. Senior management team reviews value delivery and risks related to IT. Spending on IT is based on a mixture of value and risk metrics.  
                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Level 5              | **Optimized and balanced procedures and practices**  
Senior management has enough information about IT to make informed business decisions without being personally involved in “running IT.” IT activities are optimally directed to deliver business value and avoid business risk, both of which are measured, with backup plans to correct deviations and problems. Continuous Quality Improvement programs are implemented to consistently measure deviations from objectives. Continuous improvement of prioritized IT capabilities is embedded and benchmarked against internal and external metrics, as well as internal and external audit results. Spending on IT is optimized and changed to deliver the greatest value at a risk appropriate for the organization.  
                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

Table 1. GRC CMM maturity spectrum  
*Source: IT Policy Compliance Group, 2008*
Improving business results and mitigating financial risk

Learning and growth

- IT process frameworks: ISO, ITIL, SDLC, CobiT, PCI
- Procedural (manual) controls
- Employee education/training
- Automated (technical) controls
- Policy-in, audit log-out
- Machine controls and CIS benchmarks
- Employee notification and certification

Common IT procedures

- New technology capabilities
- Change to existing capabilities
- M&A
- Vendor management

Financial

- Balanced scorecard
- Vision and strategy
- Business procedures

Business risks

- Policies and control objectives

Assess

- Improve

- Measure

Assess

- Improve

- Measure

Customers

Portfolio management

- Business rewards
- Business procedures

Assess

- Improve

- Measure

Portfolio management

- Project and risk management

Assess

- Improve

- Measure

Project and risk management

Portfolio management

Business rewards

Balanced scorecard

Vision and strategy

Business procedures

Business rewards

Policies and control objectives

Figure 47. Organizational competency: Integrated IT GRC
Source: IT Policy Compliance Group, 2008
Improving business results and mitigating financial risk

Table 2. Organizational competencies among the most mature
Source: IT Policy Compliance Group, 2008

- Senior management involvement
- Audit committee involvement
- IT, legal, internal audit, and finance leadership
- Employee training and a culture of compliance
- Improvements to IT risk assessments, data protection, IT audit, risk, and compliance practices and capabilities
- Adjustments to spending in IT to support needed capabilities
- A Continuous Quality Improvement program for IT GRC
- An integrated IT GRC program

Table 3. Practices and capabilities among the most mature
Source: IT Policy Compliance Group, 2008

- Access to sensitive and protected data on PCs and laptops is segmented and protected.
- Meaningful and measurable control objectives and policies are employed, based on business risks.
- IT policies, process frameworks, and control objectives are mapped to one another.
- Common IT procedures are employed for audit.
- Three times more controls than objectives are employed.
- Consistent configurations and common IT procedures are employed.
- Automation is widely employed.
  - 50 percent of all controls are technical controls and 100 percent of these are automated.
  - Specific IT activities are automated.
- Policy-in and audit-out for technical controls is managed.
- IT change controls and unauthorized change prevention are implemented.
- Monitoring, measurement, and reporting occur from continuously to once a month.
## Table 4. Culture, budgeting, and spending
*Source: IT Policy Compliance Group, 2008*

<table>
<thead>
<tr>
<th>Culture and budgeting</th>
<th>Level 0</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>View of IT contribution to the organization</td>
<td>Not measured</td>
<td>IT is viewed as a utility expense and structured as such.</td>
<td>IT is primarily viewed as a utility expense, with specific projects for business growth.</td>
<td>IT is viewed as a utility expense and enabler of business growth.</td>
<td>IT is structured as an expense, with targets established for business growth.</td>
<td>IT is viewed as an enabler of business growth.</td>
</tr>
<tr>
<td>IT budgeting, spending, and focus</td>
<td>Not measured</td>
<td>IT spending is done from business units only.</td>
<td>Business units retain ownership of major applications. IT is responsible for infrastructure.</td>
<td>Most IT spending on IT is done by central IT headquarters only.</td>
<td>Business units purchase from vetted lists and IT is responsible for maintaining existing services.</td>
<td>Spending and budgets for IT are shared between business units and IT headquarters based on balanced scorecard.</td>
</tr>
</tbody>
</table>

## Table 5. Business metrics, financial rewards, and risks
*Source: IT Policy Compliance Group, 2008*

<table>
<thead>
<tr>
<th>Business outcomes</th>
<th>Level 0</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer satisfaction</td>
<td>Not measured</td>
<td>8.7% lower</td>
<td>4.4% lower</td>
<td>No change</td>
<td>4.4% higher</td>
<td>8.7% higher</td>
</tr>
<tr>
<td>Customer retention</td>
<td>Not measured</td>
<td>6.3% lower</td>
<td>3.7% lower</td>
<td>No change</td>
<td>3.7% higher</td>
<td>7.3% higher</td>
</tr>
<tr>
<td>Revenues</td>
<td>Not measured</td>
<td>8.5% lower</td>
<td>4.3% lower</td>
<td>No change</td>
<td>4.3% higher</td>
<td>8.5% higher</td>
</tr>
<tr>
<td>Expenses</td>
<td>Not measured</td>
<td>6.4% lower</td>
<td>3.2% lower</td>
<td>No change</td>
<td>3.2% higher</td>
<td>6.4% higher</td>
</tr>
<tr>
<td>Profits</td>
<td>Not measured</td>
<td>6.9% lower</td>
<td>3.5% lower</td>
<td>No change</td>
<td>3.5% higher</td>
<td>6.9% higher</td>
</tr>
</tbody>
</table>

## Table 6. Financial losses and risks
*Source: IT Policy Compliance Group, 2008*

<table>
<thead>
<tr>
<th>Loss and risk</th>
<th>Level 0</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capital loss from data loss or theft</td>
<td>Approaches 10% of revenue, depending on firm size</td>
<td>Around 8% of revenue, depending on firm size</td>
<td>Around 6.5% of revenue, depending on firm size</td>
<td>Around 5% of revenue, depending on firm size</td>
<td>Around 3% of revenue, depending on firm size</td>
<td>Around 0.5% of revenue, depending on firm size</td>
</tr>
<tr>
<td>Frequency of capital loss from the loss or theft of sensitive data</td>
<td>Once every half-year to once every 10 years, depending on firm size</td>
<td>Once every year to once every 16 years, depending on firm size</td>
<td>Once every year to once every 25 years, depending on firm size</td>
<td>Once every 1.5 years to once every 45 years, depending on firm size</td>
<td>Once every 2.5 years to once every 77 years, depending on firm size</td>
<td>Once every 13 years to once every 800 years, depending on firm size</td>
</tr>
<tr>
<td>Capital loss from IT-based business disruptions</td>
<td>3–30% of revenue, depending on operational impact</td>
<td>1–9% of revenue, depending on operational impact</td>
<td>0.4–4% of revenue, depending on operational impact</td>
<td>0.1–1% of revenue, depending on operational impact</td>
<td>0.08–0.8% of revenue, depending on operational impact</td>
<td>0.03–0.3% of revenue, depending on operational impact</td>
</tr>
</tbody>
</table>
### Table 7. Business and financial risk indicators

*Source: IT Policy Compliance Group, 2008*

<table>
<thead>
<tr>
<th>Indicators</th>
<th>Level 0</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of annual losses or thefts of sensitive data annually</td>
<td>16 or more</td>
<td>12</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>2 or less</td>
</tr>
<tr>
<td>Number of business disruptions based on IT service disruptions</td>
<td>24 or more</td>
<td>14</td>
<td>9</td>
<td>5</td>
<td>4</td>
<td>2 or less</td>
</tr>
<tr>
<td>Hours to resume business operations after IT service disruptions</td>
<td>28 or more</td>
<td>14</td>
<td>8</td>
<td>5</td>
<td>4</td>
<td>3 or less</td>
</tr>
<tr>
<td>Total hours of downtime annually</td>
<td>672 or more</td>
<td>196</td>
<td>72</td>
<td>25</td>
<td>16</td>
<td>6 or less</td>
</tr>
<tr>
<td>Regulatory compliance deficiencies to correct to pass audit</td>
<td>16 or more</td>
<td>12</td>
<td>10</td>
<td>8</td>
<td>4</td>
<td>2 or less</td>
</tr>
</tbody>
</table>

### Table 8. Third-party, outsourced, and offshored IT services

*Source: IT Policy Compliance Group, 2008*

<table>
<thead>
<tr>
<th>IT services</th>
<th>Level 0</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maturity by percentage of IT services performed by third-party vendors,</td>
<td>Not measured</td>
<td>Between 40% and 60% of all IT services are outsourced or offshored.</td>
<td>Between 60% and 80% of all IT services are outsourced or offshored.</td>
<td>Between 80% and 100% of all IT services are outsourced or offshored.</td>
<td>Between 20% and 40% of all IT services are outsourced or offshored.</td>
<td>Between 0% and 20% of all IT services are outsourced or offshored.</td>
</tr>
<tr>
<td>outsourced, or offshored</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 9. Continuous Quality Improvement

*Source: IT Policy Compliance Group, 2008*

<table>
<thead>
<tr>
<th>CQI</th>
<th>Level 0</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existence and completeness of CQI programs</td>
<td>Not measured</td>
<td>CQI is nonexistent</td>
<td>CQI is nonexistent.</td>
<td>CQI program implemented in ad-hoc fashion and not connected with business results.</td>
<td>CQI program implemented by senior management team for major business initiatives.</td>
<td>Integrated CQI program is implemented from balanced scorecard through operations.</td>
</tr>
</tbody>
</table>
Improving business results and mitigating financial risk

<table>
<thead>
<tr>
<th>Behavior and usage within IT operations, IT assurance, and IT audit</th>
<th>Maturity level 1</th>
<th>Maturity level 2</th>
<th>Maturity level 3</th>
<th>Maturity level 4</th>
<th>Maturity level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Four to five different frameworks are consulted but none are adopted as standards for use with IT operations, IT assurance, and IT audit.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Two to three different frameworks are consulted as the organization narrows down what it considers “best practices” for use with IT operations.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization attempts to standardize on one to two industry frameworks for use with IT operations, IT assurance, and IT audit.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List of frameworks is expanded to develop own framework to more effectively manage challenges within IT operations, IT assurance, and IT audit.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Own framework for IT operations, IT assurance, and IT audit is mapped to four or five different frameworks for managing risk, regulatory compliance, and business rewards.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Behavior within IT management</th>
<th>Maturity level 1</th>
<th>Maturity level 2</th>
<th>Maturity level 3</th>
<th>Maturity level 4</th>
<th>Maturity level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>None are consulted or adopted.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project management skills are emphasized, but no framework adoption occurs.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Frameworks for project management are adopted to deliver technology solutions.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Frameworks for business management, project management, and portfolio management are implemented to manage business rewards.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Frameworks for business management, project management, portfolio management, capability management, and quality improvement are implemented to balance reward and risk.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 10. Behavior and use of frameworks

Source: IT Policy Compliance Group, 2008

<table>
<thead>
<tr>
<th>Training and education about company policies</th>
<th>Maturity level 1</th>
<th>Maturity level 2</th>
<th>Maturity level 3</th>
<th>Maturity level 4</th>
<th>Maturity level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is left to the discretion of hiring managers.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is delivered to employees upon hiring and documented in employee handbook.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is delivered to all employees as part of onsite and required manager training programs, and is typically delivered once per year.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New programs dealing with legal and regulatory requirements are delivered as part of core curriculum. Delivery method starts to include Web- and computer-assisted training.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Formalized training program is implemented with Web- and computer-assisted course and policy curriculum, with multiple courses delivered every year.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 11. Employee training and education

Source: IT Policy Compliance Group, 2008
<table>
<thead>
<tr>
<th>Maturity level 1</th>
<th>Maturity level 2</th>
<th>Maturity level 3</th>
<th>Maturity level 4</th>
<th>Maturity level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary focus areas for employee training</td>
<td>Ethics and code of conduct</td>
<td>Ethics and code of conduct</td>
<td>Ethics and code of conduct</td>
<td>Ethics and code of conduct</td>
</tr>
<tr>
<td></td>
<td>Handling conflicts of interest</td>
<td>Discrimination and harassment</td>
<td>Regulatory policies and procedures</td>
<td>IT compliance, security, and data protection policies</td>
</tr>
<tr>
<td></td>
<td>IT compliance, security, and data protection policies</td>
<td>IT compliance, security, and data protection policies</td>
<td>Discrimination and harassment</td>
<td>Discrimination and harassment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Discrimination and harassment</td>
<td>Handling conflicts of interest</td>
<td>Handling conflicts of interest</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Financial reporting and insider trading</td>
<td>Emergency response and restoration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Financial reporting and insider trading</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Handling legal requests and summonses for information</td>
</tr>
</tbody>
</table>

Table 12. Employee training and education
Source: IT Policy Compliance Group, 2008

<table>
<thead>
<tr>
<th>Maturity level 1</th>
<th>Maturity level 2</th>
<th>Maturity level 3</th>
<th>Maturity level 4</th>
<th>Maturity level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spending on IT assurance and audit as a percentage of the IT budget</td>
<td>5.2% to 7.4%</td>
<td>6.4% to 8.6%</td>
<td>7.4% to 9.6%</td>
<td>8.6% to 10.6%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>9.6% to 11.6%</td>
</tr>
</tbody>
</table>

Table 13. Spending on IT assurance and audit
Source: IT Policy Compliance group, 2008
<table>
<thead>
<tr>
<th>Maturity level 1</th>
<th>Maturity level 2</th>
<th>Maturity level 3</th>
<th>Maturity level 4</th>
<th>Maturity level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Actions taken to improve control objectives for IT GRC</strong></td>
<td>Audit-based to pass the primary audit.</td>
<td>Audit-based to pass multiple audits.</td>
<td>Mixture of organizational policies to pass multiple audits.</td>
<td>Common policies and control objectives across multiple audits.</td>
</tr>
<tr>
<td><strong>Actions taken to improve controls for IT GRC</strong></td>
<td>Dominant manual and procedural controls to pass audit are documented.</td>
<td>Manual procedures and controls are rationalized against policies and control objectives.</td>
<td>Manual and technically automated procedures and controls for highest business risks are identified.</td>
<td>Mix of manual, procedural, and technical controls is changed.</td>
</tr>
<tr>
<td><strong>Organizational actions taken to improve IT GRC results</strong></td>
<td>Evidence about conformance with policies is gathered to pass the primary audit.</td>
<td>Evidence about conformance with policies is gathered to pass multiple audits.</td>
<td>Self-assessments of procedural controls are conducted.</td>
<td>Self-assessments of procedural controls are conducted.</td>
</tr>
<tr>
<td></td>
<td>Gaps in procedures and IT general controls are fixed to pass audit.</td>
<td>Gaps in procedural controls and IT general controls are fixed to pass multiple audits.</td>
<td>Gaps in procedures and IT general controls are fixed to pass audit.</td>
<td>Monitoring and measurement of technical controls are being automated.</td>
</tr>
<tr>
<td></td>
<td>Rules and responsibilities of policy owners are established.</td>
<td>Rules and responsibilities of policy owners are established.</td>
<td>Rules and responsibilities of policy owners are established.</td>
<td>Gaps in procedural controls and IT general controls are fixed to pass multiple audits.</td>
</tr>
<tr>
<td></td>
<td>Self-assessments of mostly manual procedural controls are conducted to pass audits.</td>
<td>Self-assessments of mostly manual procedural controls are conducted to pass audits.</td>
<td>Evidence about conformance with policies is gathered to pass audits.</td>
<td>Policy owners are responsible for authorizing access to IT resources and employee training is a mix of electronic, paper, and instructor-led.</td>
</tr>
<tr>
<td></td>
<td>Employee training is left to individual managers.</td>
<td>Employee training is paper-based in employee manuals.</td>
<td>Employee training is paper-based in employee manuals.</td>
<td>Employee training is a mix of electronic, paper, and instructor-led.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 14. Actions to improve results**

*Source: IT Policy Compliance Group, 2008*
## Improving business results and mitigating financial risk

<table>
<thead>
<tr>
<th>Maturity level 1</th>
<th>Maturity level 2</th>
<th>Maturity level 3</th>
<th>Maturity level 4</th>
<th>Maturity level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of control objectives</td>
<td>82</td>
<td>70</td>
<td>58</td>
<td>45</td>
</tr>
<tr>
<td>Basis for control objectives</td>
<td>An amalgam of audit control statements, recommendations from auditors, and financial reporting risks.</td>
<td>An amalgam of audit control statements, recommendations from auditors, and financial reporting risks.</td>
<td>A mixture of recommendations from internal audit, finance, and IT.</td>
<td>A mixture of recommendations from internal audit, IT audit, IT assurance, and legal.</td>
</tr>
<tr>
<td>Number of controls</td>
<td>45</td>
<td>60</td>
<td>76</td>
<td>95</td>
</tr>
<tr>
<td>Proportion of manual controls</td>
<td>72%</td>
<td>66%</td>
<td>60%</td>
<td>53%</td>
</tr>
<tr>
<td>Proportion of automated technical controls</td>
<td>28%</td>
<td>34%</td>
<td>40%</td>
<td>47%</td>
</tr>
<tr>
<td>Proportion of technical controls that are fully automated</td>
<td>3%</td>
<td>8%</td>
<td>23%</td>
<td>49%</td>
</tr>
<tr>
<td>Basis for controls</td>
<td>Whatever manual procedures and technical controls are available and recommendations of auditors.</td>
<td>Whatever manual procedures and technical controls are available and recommendations of auditors.</td>
<td>Business risks from internal audit, finance, IT, and recommendations of auditors.</td>
<td>Consensus of business risks from leadership and audit committee.</td>
</tr>
</tbody>
</table>

**Table 15. Policies, objectives, and controls**

*Source: IT Policy Compliance Group, 2008*
## Frequency of measurement, assessment, and reporting

<table>
<thead>
<tr>
<th>Maturity level</th>
<th>Maturity level 1</th>
<th>Maturity level 2</th>
<th>Maturity level 3</th>
<th>Maturity level 4</th>
<th>Maturity level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency of IT general controls assessment, measurement, monitoring, and reporting for regulatory audit</td>
<td>Once every 300 days</td>
<td>Once every 222 days</td>
<td>Once every 105 days</td>
<td>Once every 45 days</td>
<td>Once every 17 days</td>
</tr>
<tr>
<td>Frequency of IT general controls assessment, measurement, monitoring, and reporting for data protection</td>
<td>Once every 300 days</td>
<td>Once every 210 days</td>
<td>Once every 90 days</td>
<td>Once every 29 days</td>
<td>Once every 4 days</td>
</tr>
<tr>
<td>Percentage of IT general controls routinely assessed, measured, monitored, and reported</td>
<td>30%</td>
<td>40%</td>
<td>50%</td>
<td>60%</td>
<td>70%</td>
</tr>
</tbody>
</table>

*Table 16. Frequency of measurement, assessment, and reporting*

*Source: IT Policy Compliance Group, 2008*

## Change management and prevention

<table>
<thead>
<tr>
<th>Maturity level</th>
<th>Maturity level 1</th>
<th>Maturity level 2</th>
<th>Maturity level 3</th>
<th>Maturity level 4</th>
<th>Maturity level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT change management program</td>
<td>Change management for IT is not considered a priority or is unknown.</td>
<td>Change management is limited to PCs and financial systems to pass audits.</td>
<td>Change management is implemented for critical IT resources.</td>
<td>Change management is implemented for all IT resources.</td>
<td></td>
</tr>
<tr>
<td>Unauthorized changes to IT resources automatically prevented</td>
<td>25%</td>
<td>35%</td>
<td>45%</td>
<td>60%</td>
<td>75%</td>
</tr>
<tr>
<td>Unauthorized changes to IT resources managed by exception</td>
<td>75%</td>
<td>65%</td>
<td>55%</td>
<td>40%</td>
<td>25%</td>
</tr>
</tbody>
</table>

*Table 17. Change management and prevention*

*Source: IT Policy Compliance Group, 2008*
Appendix B: Results by industry and size

Industry results

A firm’s operation in a more highly regulated industry is not a guarantee of better IT GRC results. Among more than 41 industries, those with marginally worse results than the market at large include:

- Banking
- Financial and accounting services
- Government and public administration

Although the benchmarks show that the IT GRC maturity of firms in most industries are in line with all other organizations, banking, government (public administration), and financial services (including accounting services) have proportionately more firms operating at the least mature level for IT GRC than the general industry (see Figure 48).

![Industry Results Diagram](image-url)

**Figure 48. Industry results**

*Source: IT Policy Compliance Group, 2008*
Rather than 20 percent of the population performing at the least mature levels, these industries (banking, financial services, and government public administration agencies) have 25 percent, 26 percent, and 29 percent respectively performing at the least mature levels.

Among banks, marginally more perform better than the industry average, with 14 percent among the most mature. The difference, 61 percent, shows that fewer banks are performing at the norm when compared with the industry average.

Among financial services firms, 14 percent are performing better than the industry average among the most mature. The difference, 60 percent, shows fewer financial services firms are performing at the industry norm when compared with the industry average for normative performers at 68 percent of the population.

Among all civil government agencies, from large to small, the population performing at the most mature levels numbers just 10 percent, 2 percent less than the industry average. The difference, 61 percent, shows fewer government agencies are performing at the industry average for normative IT GRC results.

In addition, there are far more normative performers for IT GRC among firms in architecture, construction, engineering, and legal services, with 83 percent and 78 percent of these firms among the normative performers for IT GRC.

Other industries

Although not yet reliable due to smaller sample sizes, early results indicate the industries with significant variation from industry averages include the following:

- Aerospace, with about 3 in 10 firms being among the most mature
- Telecommunications services, with about 3 in 10 firms being among the least mature
- Travel, accommodation, and hospitality services, with about 8 in 10 firms being in the norm
- Utilities, with about 8 in 10 firms being in the norm
- Computer software and services, with about 8 in 10 firms being in the norm
- Wholesale trade, with about 8 in 10 firms being in the norm

The research shows there is no advantage accruing to a company due to the regulatory nature of the industry in which the firm competes. Rather, it is the actions, practices, and capabilities that are employed for IT GRC maturity that are making the difference to business results and financial risks.
Large enterprises: Slightly more at risk

Similar to industry results, most organizations of varying size, as measured by annual revenues or annual budget, are performing in line with the industry averages for IT GRC, with 20 percent operating at the least mature level, 68 percent at norm and 12 percent operating at the most mature levels.

However, the variation among large firms (those with more than $1 billion in revenue) shows more of these firms—28 percent—are operating at the least mature levels for IT GRC maturity. This is 8 percent above average when compared with 20 percent for all firms. The number of large enterprises operating at the norm numbers 58 percent of all large firms, down significantly from the industry average of 68 percent. The difference, 14 percent, indicates that a smaller set of the largest firms are operating above the industry average with the most mature IT GRC profiles (see Figure 49).

These results are in line with related research that shows large firms make up the bulk of the population that finds Sarbanes-Oxley the most pressing regulatory mandate for the organization, and similar results showing the dominant framework of choice for IT GRC among the least mature is either ITIL or CobiT, as well as the results for control objectives showing larger enterprises with an average of 75 control objectives, 2.5 times more than is ideal.

The combination of larger financial exposure, and more frequent loss or theft of customer data, means that a proportionally larger number of firms among those with $1 billion or more in revenue are more at risk than midsize and small businesses within the same industry.
About the benchmarks

Topics researched by the IT Policy Compliance Group (IT PCG) benchmarks are part of an ongoing research calendar established by input from supporting members, advisory members, and general members of the Group, as well as from findings compiled from ongoing research.

This annual report includes research findings that date back one quarter, two quarters, one year, and even two years ago. The aggregation of findings across multiple research studies has only been conducted where all the findings for specific tracking questions are identical, or where the analysis of variance shows the findings within and across all of the benchmarks are within the population means and standard deviations.

The most recent benchmarks included in this report were conducted between December 2007 and March 2008 with 558 separate, qualifying organizations. The consistent findings related to tracking questions from earlier benchmarks conducted between June 2007 and March 2008 with up to 2,608 separate firms have been included, but only where errors do not skew results of findings.

The majority of the organizations (90 percent) participating in the benchmarks are located in North America and the remaining ten percent of the participants for the research findings come from countries located in Africa, Asia Pacific, Europe, the Middle East and South America.

Although the majority of participants hail from North America, many members of the Group from outside this geography have, through separate communications, indicated that the results cited apply equally well within their organizations that happen to be located in other industrialized and rapidly industrializing geographies from around the world. As a result, the Group believes the findings related to the maturity of IT GRC practices and business outcomes that are cited in this report are applicable to most organizations and areas of the world where IT services are embedded as part of common business procedures.

In addition to specific tracking questions common to each benchmark, the benchmarks are also designed to uncover the relationship between business results, the actions that organizations have taken in response to business pressures, and the capabilities these organizations have to respond to business pressures.

Industries represented

Almost every industry has participated in the benchmark, including accounting services, advertising, aerospace, agriculture, apparel, architecture, automotive, banking, chemicals, computer equipment and peripherals, computer software and services, construction, consumer durable goods, consumer electronics, consumer packaged goods, distribution, education, engineering services, financial services, general business and repair services, government (public administration), government (defense and intelligence), health, medical and dental services, insurance, law enforcement, legal services, management services, scientific and consulting services, manufacturing, medical devices, metals and metal products, mining, oil and gas, paper, timber and lumber, pharmaceuticals, public relations, publishing, media and entertainment, real estate, rental and leasing services, retail trade, telecommunications equipment, telecommunication services, transportation and warehousing, travel, accommodation and hospitality services, utilities, and wholesale trade. Manufacturing accounts for roughly twelve percent of participating organizations. All other industries account for less than ten percent of the benchmark participants.
Revenue of participating organizations

Thirty-three percent of the organizations participating in the benchmark have annual revenues, assets under management, or budgets that are less than $50 million. Another 31 percent have annual revenues, assets under management, or budgets that are between $50 million and $999 million. The remaining 36 percent have annual revenues, assets under management, or budgets that are $1 billion or more.

Number of people employed by participating organizations

Thirty percent of the participating organizations employ less than 250 people. Twenty-nine percent employ between 250 and 2,499 people. The remaining 41 percent employ 2,500 or more people.

Job titles of participants

Twenty-eight percent of the participants in the benchmark are senior managers (CEO, CFO, CIO, and so on), 13 percent are vice presidents, 34 percent are managers or directors, 24 percent are staff, and 1 percent work as internal consultants.

Roles of participants

Thirty-two percent of the participants work in IT, another 27 percent work in finance and internal controls, 15 percent work in legal and compliance, 5 percent work in sales and marketing, 5 percent work in product design and development, and the remaining 16 percent of the participants work in a wide range of job functions, including customer service, manufacturing, procurement, and logistics.

About IT Policy Compliance Group

The IT Policy Compliance Group is dedicated to promoting the development of research and information that will help organizations meet their policy and regulatory compliance goals. The IT Policy Compliance Group focuses on assisting member organizations to improve business, governance, risk management, and compliance results based on fact-based benchmarks.

The IT Policy Compliance Group Web site at www.itpolicycompliance.com features content by leading experts in the world of compliance and published reports containing primary research. Research benchmarks and interactive assessment tools sponsored by the Group deliver fact-based insight and recommendations about what is working and why, and what can be done to improve results.

The Group’s research is designed to help legal, financial, internal controls, and professionals to:

• Benchmark results and efforts against peers and best-in-class performers
• Identify key drivers, challenges, and responses to improve results
• Determine the applicability and use of specific capabilities to improve results
• Identify best practices for IT governance, risk, and compliance

The Group relies upon its supporting members, advisory members, associate members, and significant benchmark findings to drive its research and editorial calendar.
IT Policy Compliance Group Supporters

**Symantec Corporation**
20330 Stevens Creek Blvd.
Cupertino, CA 95014
+1 (408) 517 8000
www.symantec.com
info@symantec.com

**Computer Security Institute**
600 Harrison St.
San Francisco, CA 94107
+1 (415) 947 6320
csi@cmp.com
www.gocsi.com

**The Institute of Internal Auditors**
247 Maitland Ave.
Altamonte Springs, FL 3270-4201
+1 (407) 937 1100
iiia@theiia.org
www.theiia.org

**Protiviti**
1290 Avenue of the Americas,
5th Floor
New York, NY 10104
+1 (212) 603 8300
info@protiviti.com
www.protiviti.com

**Information Systems Audit and Control Association**
3701 Algonquin Rd., Suite 1010
Rolling Meadows, IL 60008
+1 (847) 253 1545
info@isaca.org
www.isaca.org

**IT Governance Institute**
3701 Algonquin Rd., Suite 1010
Rolling Meadows, IL 60008
+1 (847) 660 5600
info@itgi.org
www.itgi.org

**Symantec Corporation**
20330 Stevens Creek Blvd.
Cupertino, CA 95014
+1 (408) 517 8000
www.symantec.com
info@symantec.com

© 2008 IT Policy Compliance Group
Founded in 2005, the IT Policy Compliance Group conducts benchmarks that are focused on delivering fact-based guidance on steps that can be taken to improve results. Benchmark results are reported through www.itpolicycompliance.com for the benefit of members.

IT Policy Compliance Group

Contact: Managing Director, Jim Hurley
Telephone: +1 (216) 321 7864
Jhurley@itpolicycompliance.com
www.itpolicycompliance.com

May 2008