

IT GOVERNANCE, RISK AND COMPLIANCE 2008 ANNUAL REPORT

Key Findings

IT governance, risk and compliance (IT GRC) is about striking an appropriate balance between business reward and risk. The maturity of IT GRC practices for managing reward and risk has a direct impact on the organization. The 2008 Annual Report reveals the competencies, capabilities and practices that are most responsible for influencing and impacting business rewards and risks.

IT GRC encompasses the practices for delivering:

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


Primary benchmark research conducted by the IT Policy Compliance Group (IT PCG) indicates that the way to improve business results, 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.

The research has resulted in a GRC Capability Maturity Model (GRC CMM) Derived from firms with specific business results, the practices, capabilities and competencies in the GRC CCM deliver empirical insight into what is working, and not working, based on primary research and facts, not hypothesis.

The evidence from the benchmarks show an almost one-to-one relationship between actions and practices implemented by an organization to improve GRC maturity with better business results and less business risk.

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.

Business Results and IT GRC Maturity

Least mature  Most mature

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

Implications and Analysis

Only slightly more than one-in-ten firms enjoy the business benefits associated with the most mature IT GRC practices including:

- 17 percent higher revenues than all other firms
- 14 percent higher profits than all others
- 18 percent higher customer satisfaction rates
- 17 percent higher customer retention levels
- 96 percent lower financial losses from the loss of theft of customer data
- 50 times less likely to lose or have stolen customer data
- 50 percent less spent on regulatory compliance annually

To improve business results, reduce risk, loss and expense, organizations need to increase or enhance the IT GRC competencies, practices and organizational competencies implemented by the most mature firms include:

- Greater senior management involvement
- Involvement by the audit committee
- Leadership by IT, legal, audit and finance functions
- Employee training and a culture of compliance
- Improvement 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

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

- Access to sensitive data and protection of data on PCs and laptops is segmented and limited
- Meaningful and measurable control objectives and policies based on business risk are employed
- IT policies, process frameworks and objectives are mapped to one another
- Common IT procedures are employed for audit
- Three times more controls are employed than objectives
- Consistent configurations and common IT procedures are employed
- Automation is widely used
 - 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 control and unauthorized change prevention are implemented
- Monitoring, measurements and reporting occur between continuously to once a month

Recommendations for Action

Based on the benchmark findings, recommendations include the following.

Procedure for Improving IT GRC Practices

- Assess the current maturity state of the organization
- Determine the business and financial outcomes from the current maturity profile
- Identify desired maturity, agility, quality, financial and compliance objectives
- Identify the practices and capabilities needed to achieve desired objectives
- Qualify and quantify expected costs, savings and financial risks
- Implement the quality improvements to achieve objectives
- Measure the results and repeat the steps

Key Recommendations

- Staff the governance committee from senior business, financial, legal, regulatory and audit committee members
- Use a Balanced Scorecard, or similar tool, to improve the delivery of value and the performance results of IT
- Drive improvements to maturing and business outcomes with measurable and continuous quality improvement program throughout IT
- Insist on monthly reporting to drive improvements
- Improve and automate technology controls to mitigate and avoid financial risk, brand damage and business disruptions
- Improve the skills and automate the activities within IT assurance, audit and risk management
- Segment and limit, where possible, to reduce exposure and costs
- Manage change management and prevention to avoid higher financial risk and cost inefficiencies
- Continuously measure and assess conditions, controls, objectives and policy to maintain an appropriate balance between reward and risk

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 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 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 firms have been included, but only where errors do not skew results from the research.

The majority of the organizations (90 percent) participating in this benchmark are located in the North America. The other 10 percent come from countries located in Africa, Asia Pacific, Europe, the Middle East and South America. Almost every industry has participated in the benchmark. Manufacturing accounted for roughly 12 percent of the participating organizations for the largest data set; all other industries account for less than ten percent of the participating organizations.

In addition to specific tracking questions common to each benchmark, the research is 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.

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. It 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 created by leading experts in the world of compliance and published reports containing primary research. Research benchmarks and interactive 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-sponsored research is designed to help legal, financial, internal controls, IT audit, IT security, and compliance 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 PCG supporters include: Symantec Corporation, The Institute of Internal Auditors, Information Systems Audit and Control Association, Computer Security Institute, Protiviti and IT Governance Institute.