Global report on the status of IT compliance processes.

GMG
Insights

AUTHORS:
Gib Trub, Managing Partner
Laurie Olski, Managing Director

TOPIC:
IT Compliance

ADDITIONAL INPUT:
James McLeod-Warrick, President
Beacon Technology Partners

PUBLICATION DATE:
October, 2008, version 2

Publishing Information

GMG Insights provides analysis, research and strategy services to companies with complex B2B sales. Publication headquarters, marketing and sales offices located at:

GMG Insights
95 Nason Hill Road
Sherborn, MA 01770
Phone: 508-545-1095
Fax: 866-725-7059
Internet: info@gmginsights.com

Methodology

This study focused on Compliance Officers, Compliance Auditors and Senior IT Management with compliance responsibility. It included a worldwide quantitative survey with a confidence level of +/- 5%. The study was conducted in April 2008.

The quantitative analysis was conducted by Beacon Technology Partners, Maynard, MA. James McLeod-Warrick, President of Beacon Technology Partners, collaborated on the analysis and reporting of the findings.

This study was sponsored by CA.

Table of Contents

Synopsis

This study examines worldwide regulatory compliance efforts and implementations in large organizations almost six years after Sarbanes-Oxley ushered in a new wave of regulations and oversight. This report provides an IT perspective on the state of compliance, attitudes, plans and market maturity.

It would seem reasonable to expect that by this time large organizations would have optimized processes and adopted technology solutions to reduce the organizational burdens of reoccurring compliance mandates and quarterly or annual audits. Surprisingly, that is uniformly not the case.

Even as the worldwide number of regulatory compliance mandates grows, the largest and most affected organizations still lack central repositories and automated systems for management and oversight. And those that have begun to automate still admit their organizational immaturity. The burden faced will only continue to grow as Europe, Asia/Pac and Central/South America continue to follow the path of North America and add additional regulatory requirements that will affect anyone doing business in these regions.

The conclusion we come to, is that in-spite of the rising costs associated with compliance and the severe penalties that can come from non-compliance, organizations are still managing down to a “just enough to get by” strategy. In our opinion this strategy cannot be sustained. Organizations face exponential growth of regulations and systems affected by those regulations must be monitored.   Managing compliance with an ad hoc approach subjects organizations to significant risks. Recognition of the organizational risk and the growing costs will ultimately drive the adoption of broader, enterprise-wide compliance management solutions.

The heavy burden of regulatory compliance is a truly global issue.

Organizations around the world must comply with a daunting array of regulations. The regulatory burden is largest in North America, where organizations with greater than $1 billion in annual revenue report they monitor an average of 45 regulations worldwide. Mid-market North American companies (less than $1 billion annual revenue) monitor an average of 19 regulations.

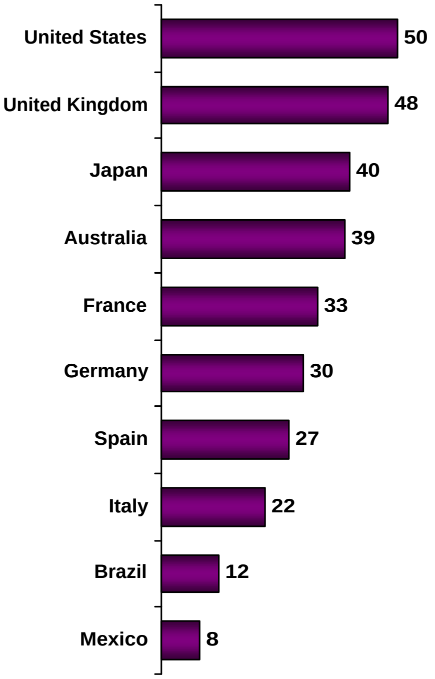


__Figure 1__*, Number of required separate regulations, by country (mean scores)*

For those operating globally, complex regulatory compliance issues exist wherever they do business. For example, 30% of European companies are required to comply with the South African King Report, while 28% of US companies are required to comply with J-SOX in Japan *(Figure 2).*

Enterprise level organizations say they comply with an average of 45 regulations

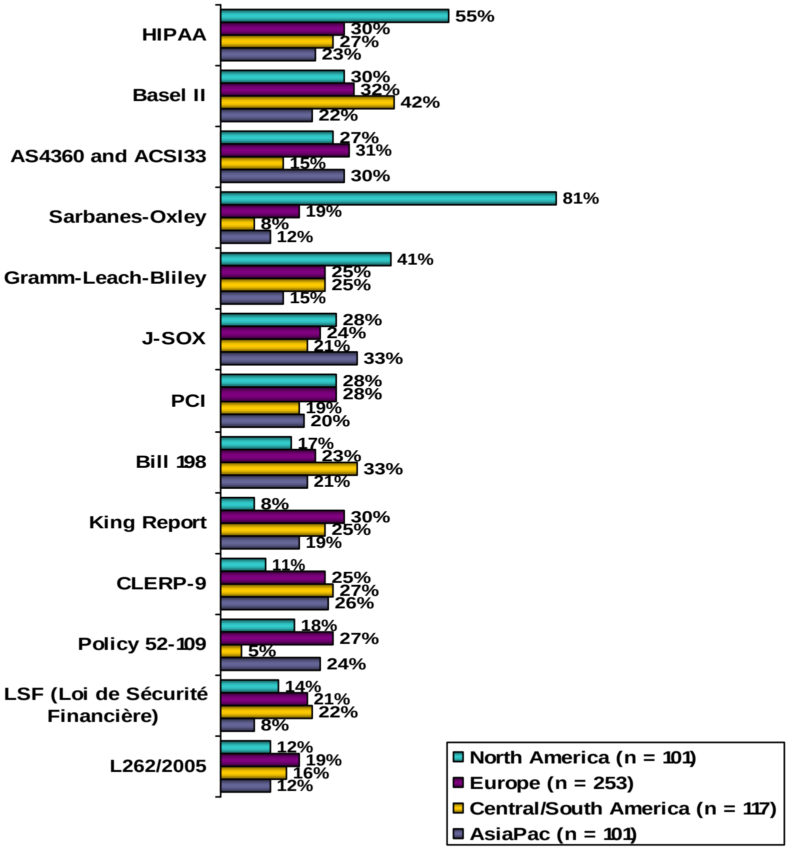
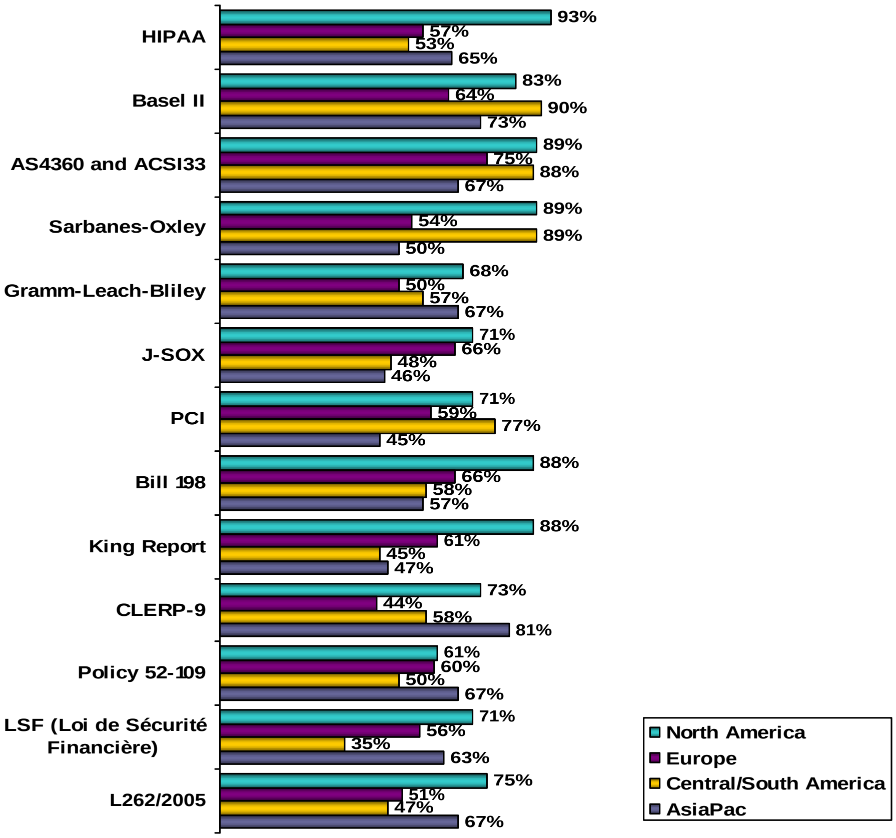


Figure 2, ***Aided reporting of regulations requiring compliance, ranked by total***

Reported organizational compliance varies on a regulation-by–regulation basis. The low rates of actual compliance with governing regulations suggest the difficulty of this global task but may also reflect that they have not yet reached the timeframe required to adhere to a regulation or a conscious effort to only pay attention to the most critical parts of the business from a regulatory standpoint. In many instances, North American organizations are more likely to be in compliance with regulations than organizations in other countries *(Figure 3)*. European, AsiaPac and especially Central/South American companies are significantly less likely to be in compliance with regulations they are subject to.

A high degree of risk associated with a particular regulation does not necessarily translate into 100% compliance. Even Sarbanes-Oxley, a high profile regulation whose significant fines and potential prison sentences reach the executive suite, has not engendered full compliance. While 89% of North American organizations required to comply with Sarbanes-Oxley report that they do so, just 50% of the AsiaPac organizations that fall within the purview of Sarbanes-Oxley report compliance *(Figure 3).*



Base= Those who must comply with each regulation

<u>Figure 3</u>, Regulations with which an organization has already complied, by region, ranked by total

The majority of companies, especially those outside the US, freely admit that they are not in compliance.

While Sarbanes-Oxley heightened the pain of compliance by initiating a new level of scrutiny, a wide array of regulations are now responsible for doing the same.
No single category of regulations is responsible for this burgeoning compliance burden. While data privacy and financial reporting are the biggest drivers, more than one-third of companies around the world are complying with environmental, securities, international trade, national security and health care regulations *(Figure 4).*

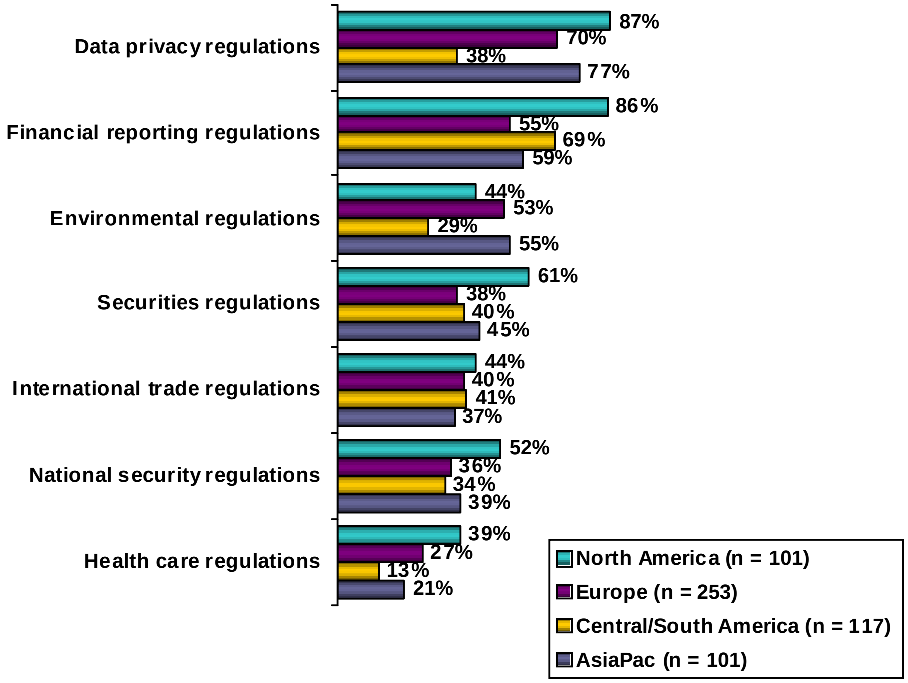


__Figure 4__*, **Topical categories of regulations by region, ranked by total.***

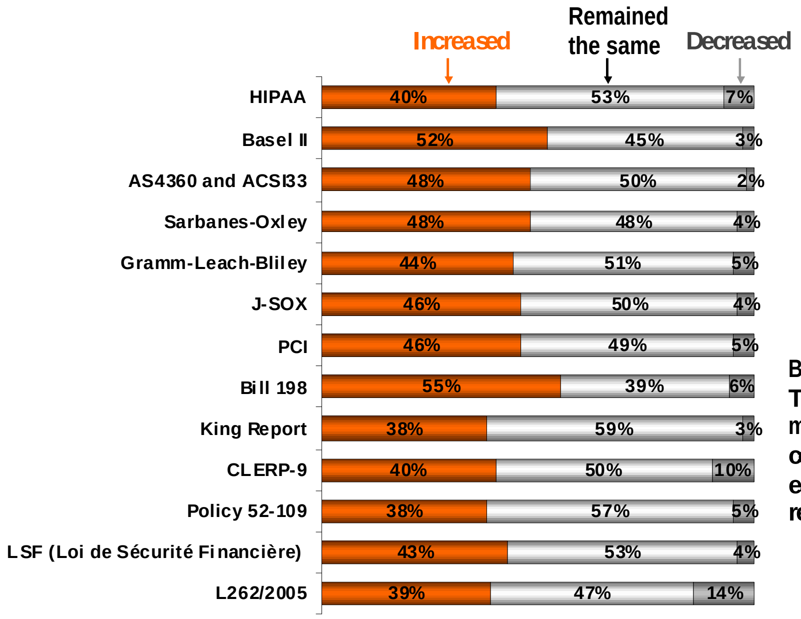
Companies in every geography are facing a broader array of regulations.

Likewise, while larger companies face a larger burden, complying with well over twice the regulations that mid-market organizations are required to, the range of regulatory issues for both is comparable.

Organizations' resource commitment to compliance grows unabated.

The growing cost of compliance is evident (*Figure 5)*. The time and money needed to achieve compliance has grown significantly year-over-year, and is likely to continue. Nearly 45% of organizations report the time and monetary resources required to ensure compliance with the regulations in *Figure 5* have increased. Less than 10% report a decrease.

Nearly 45% report the time and monetary resources required to ensure compliance has increased in the past year.



Base = Those who must comply with each regulation

Ranked by Total

Figure 5, ***Changes in total time and monetary commitments, last 12 months***

Multiple regulations are contributing to the increase in compliance costs.

Among those organizations required to comply with Sarbanes-Oxley:

- 38% perceive it to be the most expensive regulation to comply with
- 35% report it has had the biggest impact on the IT organization
- 34% believe it has had the biggest impact on overall business

Most regulations have had a similar negative impact on resources in regulated companies. IT and compliance management view the impact as both costs against budget and the cost of manhours; manhours often being the most precious.

	Most expensive	Biggest impact on IT organization	Biggest impact on overall business
	%	%	%
HIPAA	25	23	20
Basel II	24	32	27
AS4360 and ACSI33	24	30	28
Sarbanes-Oxley	38	35	34
Gramm-Leach-Bliley	25	22	16
J-SOX	19	23	18
PCI	17	14	19
Bill 198	19	20	25
King Report	17	17	22
CLERP-9	27	23	28
Policy 52-109	11	11	16
LSF (Loi de Sécurité Financière)	15	12	15

Base = Those who must comply with each regulation

48% of those surveyed report increased spending over the past year to comply with SOX.

Figure 6, ***Regulations perceived to be the most expensive, have the greatest impact***

Organizations attribute the increasing costs of compliance to many factors, including regulations and interpretations that are continually in flux.

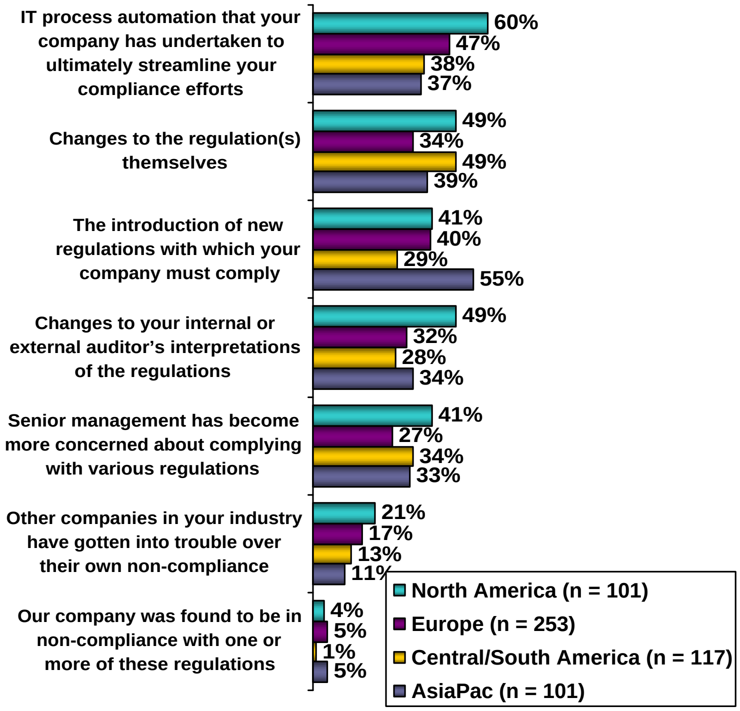


__Figure 7__, ***Reason for time and monetary increases, by region***

Regulations change every year and the auditors that assess them often have differing and evolving interpretations.

The shifting nature of regulations is a major factor in the escalating costs. In AsiaPac, 55% of organizations (where J-SOX was recently enacted), as well as 41% of North American and 40% of European organizations, report the introduction of new regulations is a reason for increasing compliance expenses. In addition, changes to internal and external auditors' regulatory interpretations are a factor in rising costs for 49% of North American organizations. Changes to the regulations themselves are also reported to be a factor by 49% of North American and Central/South American organizations, 34% of European and 39% AsiaPac organizations. These figures indicate a fluctuating environment that is likely a critical factor in the lagging rates of actual compliance.

Despite the complexity and growing burden of compliance, efforts are still largely manual.

At present more than two-thirds of the companies surveyed reported that they maintained the information about the status of their IT compliance controls in multiple spreadsheets and often with different organizational units. At least half admitted that their companies do not have central repositories to help identify the regulations and controls that directly impact them. Over 75% said that the operation, testing, monitoring and reporting of IT controls were at best a combination of automated and manual processes.

Spreadsheets pass for automation in many organizations.

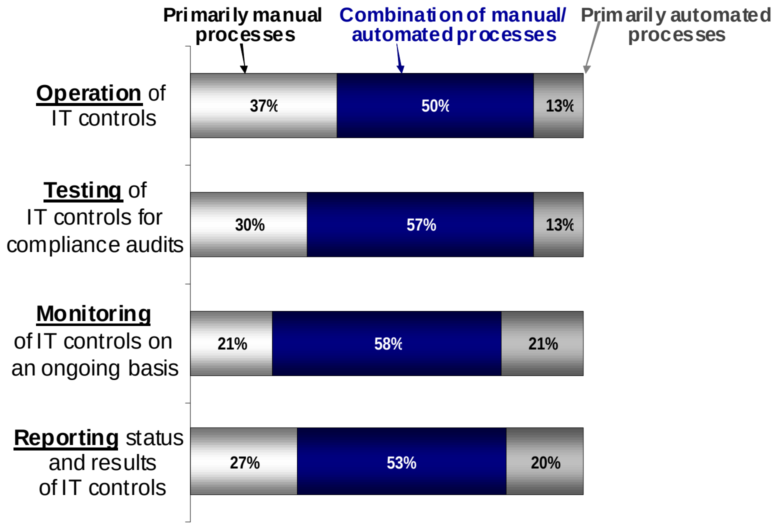


Figure 8, ***Level of automation used for IT controls, mid-market***

In an environment of increasing regulation and persistent fluctuation, manual processes and a lack of centralized control are a recipe for spiraling costs.

Some organizations are adopting best practice standards to get ahead of the compliance "curve."

The fluctuating task of ensuring compliance is difficult for companies of all sizes and industries. An effective compliance effort spans the entire organization, requiring coordination and documentation. An indication that companies are recognizing that the issue is not going away is their increasing adoption of formal methodologies like Six Sigma and ITIL. We have seen a particular rise in ITIL adoption over the last 12 months.

Interestingly there are higher rates of ITIL adoption in North America than Europe despite ITIL having its roots in Britain.

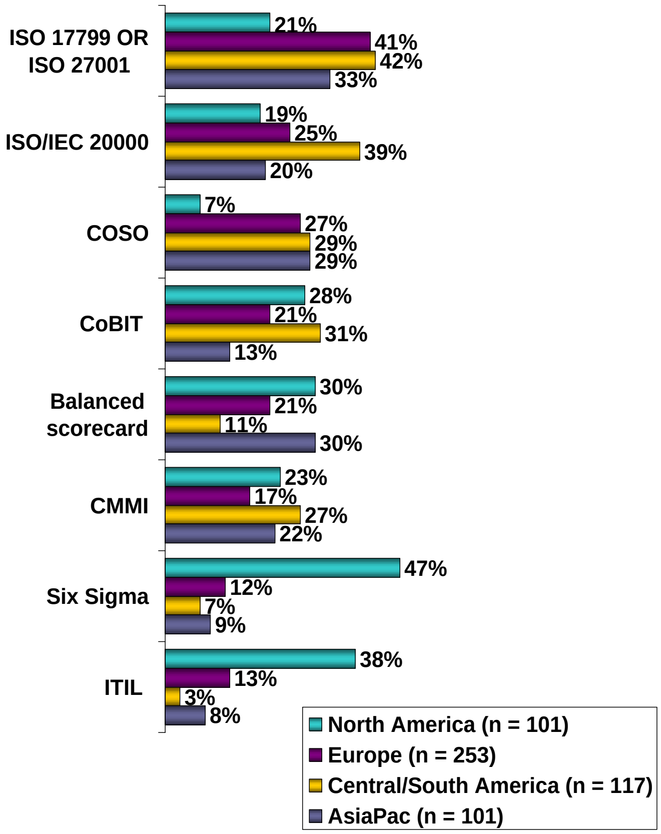


Figure 9, ***Process adoption***

38% of US companies cite compliance as the primary driver for adopting ITIL.

The first step toward compliance maturity is an organizational recognition of compliance burden and the need to standardize processes across the organization.

This survey revealed that organizations fall into one of three categories: *most mature* (15% of those companies surveyed), *along the path to maturity* (56%) and those *just getting started* (29%). Although a large percentage of the companies that were surveyed were large and faced broad regulatory responsibilities, only the most mature organizations in all regions report significant adoption of compliance processes.

Maturity indicators include adoption of best practices, seeking outside help and taking a centralized view toward establishing controls for multiple regulations rather than dealing with each on a case-by-case basis. Also, the most mature organizations are the least reliant on manual tools to achieve compliance. In fact, they are significantly more likely to have purchased IT tools and solutions to manage compliance mandates and risk exposure.

Yet even the most mature organizations have not gotten a complete organizational handle on compliance. Despite all of the measures they have taken, they still report a lack of centralized management or automation of processes, ongoing duplication of effort and manual reporting. Significant gaps in timely compliance efforts appear to be the norm. These deficiencies in compliance efforts help explain why actual rates of compliance do not vary significantly from less mature companies.

Most Mature – 15%
Tend to be large companies
Mix of manual/automated processes
Subject to an average of 49 regulations
Disproportionately North American
Highest adoption rate of best practice standards
Most likely to engage 3rd party consultants for compliance assistance
Lack of centralized management/gaps in timely compliance
81% have compliance controls to deal simultaneously with multiple regulations
Still not fully compliant

Without centralized management there is duplication of effort, increased costs, and non-compliance.

The majority of companies in all regions (50+%) are somewhere on the path to compliance maturity. However, they lack the organizational structure and support necessary to be considered mature. These companies have not yet turned to outside resources for compliance support, do not have a centralized process for identifying regulations and risk and are less likely to have senior executives whose sole focus is compliance and risk.

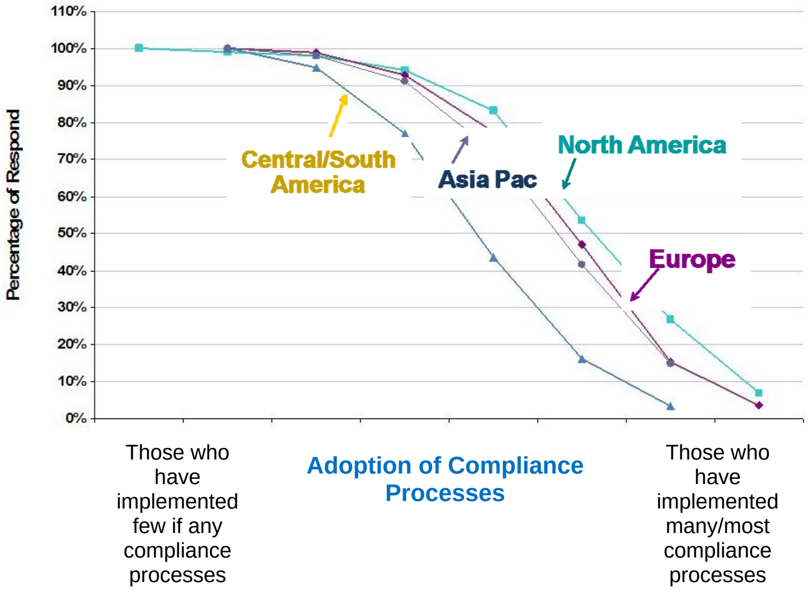
Along the Path to Compliance Maturity – 56%
Mix of large and mid-sized companies
Subject to an average of 32 regulations
More likely European
Less likely to engage 3rd party consultants than the "mature" group
More apt to report difficulty proving compliance
Some have senior execs focused on compliance and risk, but fewer than in the "mature" group

A third of the companies surveyed are barely getting started on compliance initiatives. These companies, despite confronting significant regulatory burden, are ad hoc in their approach and almost exclusively manual in their processes. They are also characterized by a lack of urgency or rigor.

Just Starting on Path to Compliance Maturity – 29%
Tend to be small companies
Mostly manual processes
Subject to an average of 24 regulations
Disproportionately Central/South American
Least likely to adopt best practice standards
Ad hoc approach to compliance efforts
IT responsible for testing compliance controls
Few have internal or external IT auditors
Furthest path to compliance

Global regions are closely tracking the evolution of North America's compliance.

The state of maturity tracks in similar fashion across all geographies except Central/South America, which is markedly behind. As would be expected, (based on the timeframe of regulatory imposition for Sarbanes-Oxley, Basel ll, et al.) North merica leads in followed by Europe and then Asia/Pac,



<u>How to read this chart</u>

This chart shows a summary spectrum of compliance implementations – using a "maturity metric" scoring methodology.

The greater the maturity score, the farther along the continuum – moving from left to right – and the fewer the number of companies that have

The data shows the difference in compliance efforts between North America and the rest of the world is rapidly shrinking.

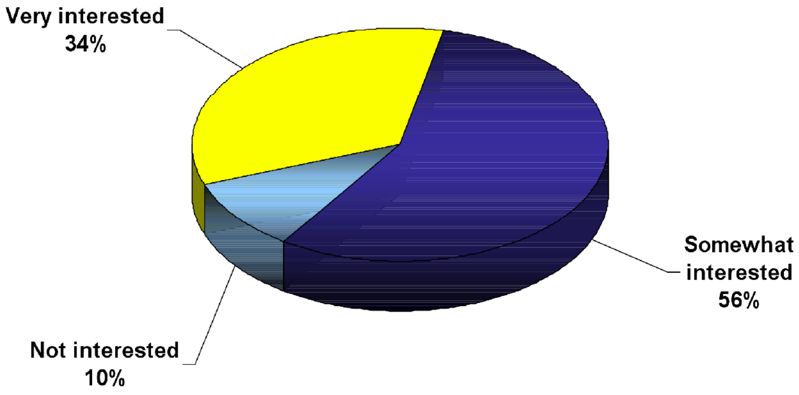
<u>Figure 10</u>, *Global maturity of compliance processes*

As this maturity model demonstrates, the vast majority of global organizations still have a long way to go in their compliance initiatives. While organizations are undertaking a variety of approaches to compliance, none have managed to wrap their arms around this shifting target.

Strong interest in automated solutions reflects the inability of most organizations to fully solve the compliance problem.

Organizations around the globe are attempting to manage the compliance process. Most have taken steps and some have begun the process of automation likely hoping to reduce errors and/or costs and refocus resources on their organizational mission. However, compliance is a growing burden, and full compliance automation is not a reality. No surprise then that this demonstrable need for a comprehensive solution has translated into clear interest in compliance solutions *(Figure 11).*

The escalating costs of compliance will force the adoption of automated software solutions.



<u>Figure 11,</u> ***Interest in compliance solutions***

Unabated growth in resources dedicated to compliance efforts will in the end lead to the adoption of better processes and software tools to aggregate and manage the process.

Prior to conducting this research, it was expected that large, sophisticated companies facing reoccurring compliance mandates and annual audits centered on long imposed regulations would have developed processes and adopted technology solutions to reduce the financial and organizational burdens of compliance. The data suggests that this is universally not the case.

This study clearly shows that large and mid-sized organizations around the world anticipate the number of regulatory compliance mandates will continue to grow. Yet the largest, most mature and most impacted organizations still lack central repositories and automated systems for management and oversight. Heavily impacted mid-sized companies are unprepared as well and have not yet made the organizational commitment to staff appropriately. The regulatory related burden will only continue to grow as the trend toward regulation proliferates globally.

In spite of the rising costs associated with compliance and the severe penalties that can come from noncompliance, organizations are still managing down to a “just enough to get by” strategy. In our opinion this strategy cannot be sustained. Organizations are subject to significant risks and costs managing with an ad hoc approach. Recognition of the organizational risk, and the growing costs, will ultimately drive the adoption of more comprehensive compliance management solutions.