Gartner Research

Publication Date: 7 July 2006 ID Number: G00138098

Understanding the Costs of Compliance

John Bace, Carol Rozwell, Joseph Feiman, Bill Kirwin

Businesses often respond to regulatory compliance issues in an ad hoc, one-off manner. This approach is less and less viable as regulatory mandates, such as those of the Sarbanes-Oxley (SOX) Act, continue to multiply. Businesses must approach compliance holistically, creating solutions that work together over the long term. This means assessing compliance practices in light of the total cost of compliance (including the company's risk exposure), coming up with effective ways of measuring the effectiveness of compliance efforts and creating a compliance governance structure that allows planning for the future.

Key Findings

- The economic impact of regulatory compliance is severe; according to the U.S. Small Business Administration, it can account for 8 percent of U.S. gross domestic product. This includes the cost of labor, opportunity cost, as well as the regulator infrastructure.
- To manage the high cost of compliance, every company must be aware of the dynamics between total cost of ownership (TCO) and compliance costs.

Predictions

- Through 2010, companies that select individual solutions for each regulatory challenge they face will spend 10 times more on the IT portion of compliance projects than companies that take a proactive and more integrated approach (0.9 probability).

Recommendations

- Combine compliance requirements and build synergistic solutions. The effort saves time and money as well as establishes a framework for responding to future requirements.
- Monitor the total cost of compliance relative to its effectiveness. Higher spending will not necessarily mean a higher level of compliance or reduction of risk.
- Understand, categorize and communicate the risks of noncompliance to your business. Agree on your preferred risk profile.
- Create a "weather bureau" to forecast changes in governance and compliance requirements.
- Create an explicit link between compliance, performance management and value.
- Manage compliance as a program, not a project. (Regulatory compliance must be continuous.)

© 2006 Gartner, Inc. and/or its Affiliates. All Rights Reserved. Reproduction and distribution of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner's research may discuss legal issues related to the information technology business, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The opinions expressed herein are subject to change without notice.

- Effective compliance requires organizational support, process control methodology and content control.
- To control compliance costs, look for commonality in compliance requirements, use an investment approach for budgeting, and take complexity out of the system whenever possible.

© 2006 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

TABLE OF CONTENTS

LIST OF FIGURES

© 2006 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

Gartner

STRATEGIC PLANNING ASSUMPTION

Through 2010, companies that select individual solutions for each regulatory challenge they face will spend 10 times more on the IT portion of compliance projects than companies that take a proactive and more integrated approach. (0.9 probability).

ANALYSIS

1.0 The High Cost of Compliance

The cost of regulatory compliance is a burden that can drain the resources out of even the most-robust and well-run business. Consider the following facts:

- W. Mark Crain and Thomas D. Hopkins, public policy researchers, estimate regulatory compliance can cost as much as $7,000 annually per employee.
- Surveys by organizations such as RHR International, a management consulting firm, and Financial Executives International, a professional society of CFOs, indicate compliance costs are two to three times higher than originally estimated because of SOX Section 404 requirements.
- Publicly held companies with revenue of less than $1 billion are spending, on average, about $1.8 million on SOX Section 404 compliance.
- According to the national law firm of Foley & Lardner, companies with revenue of less than $1 billion are spending $2.9 million on SOX compliance.
- A study conducted by CRA International for the Big Four accounting companies found first-year SOX 404 costs for public companies with revenue of more than $7 billion exceeded $8.5 million.
- Gartner's 2005 Research Compliance Survey found that IT financial compliance management spending will rise between 10 percent and 15 percent of the IT budget.

The compliance burden is not just limited to publicly held companies. A survey by Foley & Lardner of almost 300 boards of directors of privately held companies found that 77 percent were considering adopting some forms of SOX governance, control or transparency.

An October 2005 survey by Gartner found the median estimate for 2006 IT financial management compliance spending by all respondents was 15 percent of the IT budget, more than four times the 2004 estimate from the Gartner EXP CIO Insight survey. In this latest survey, the IT compliance managers estimated 10 percent of the IT budget, while CIOs said 12.5 percent and IT professionals 12 percent. The estimates for IT financial management compliance spending by audit and finance professionals were 20 percent.

The respondents to the above survey — when asked, "Which describes your 2006 IT budget planning for financial management compliance?" — 29 percent said they received an increase in their IT budget to pay for it. However, 16 percent told Gartner they deferred projects to pay for it. Another 16 percent reported taking money away for existing projects and areas, such as upgrades and technology refreshes. Six percent reported canceling some projects to pay for financial management compliance.

Another recently completed survey — the 2006 Gartner EXP CIO Survey — has found very similar results. When asked what percentage of the IT budget was being spent on compliance,

© 2006 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

more than 1,400 CIOs estimated that nearly 12 percent of their IT budget will go toward compliance. When asked where they see that number going in the future, they told us they expect that figure to grow to 14.2 percent by 2009.

The growth in IT spending that is coming out in the Gartner surveys and research analysis mirrors work done by other organizations, such as Financial Executives International (FEI). This professional society of CFOs, corporate treasurers, comptrollers and other financial executives have been doing extensive surveys during the same period, looking at total compliance costs (not just IT) for SOX. You can find their results at www.fei.org.

The economic impact of regulatory compliance is therefore severe, representing 8 percent of U.S. gross domestic product. It is estimated that "the cost of compliance" adds $8,000 per year to the cost of goods and services purchased by most U.S. households. These are costs that are related to financial compliance — for example, Occupational Safety and Health Administration (OSHA), Health Insurance Portability and Accountability Act (HIPAA) and Environmental Protection Agency (EPA) regulations — that manufacturers, distributors, retailers and service providers must pay to be in *regulatory* compliance. These costs hurt small and midsize businesses more than larger ones.

1.1 SOX and Its Impact

Compliance legislation includes but is not limited to the well-known SOX Act, the HIPAA, and the Revised International Capital Framework (Basel II). Of these, the SOX Act has received the most attention recently. Its goal is to restore investor confidence by ensuring a truly independent board of directors and more accurate, detailed financial reporting. Additionally, it calls for greater personal accountability of senior executives and adherence to new accounting standards.

Implementing SOX has been costly, with some estimating that the cost of meeting its requirements is 20 times higher than what the U.S. Securities and Exchange Commission estimated in 2003. The reasons most cited for the higher costs are: conservative interpretation of the rules by auditors: and uncertainty about what constitutes compliance, leading to frivolous actions, such as requiring auditors to sit on meetings just to prove the meetings occurred.

A survey by the Institute of Internal Auditors (IIA) revealed that 72 percent of its members found the cost of meeting Section 404 attestation exceeded the benefits "somewhat" or "greatly." However, 70 percent of respondents to the IIA study said they strongly agreed that the process directly improved monitoring and control.

2.0 Elements of Compliance Cost

2.1 Total Cost of Ownership

To manage the high cost of compliance, whether with SOX or other laws, every enterprise must be aware of the dynamics of TCO.

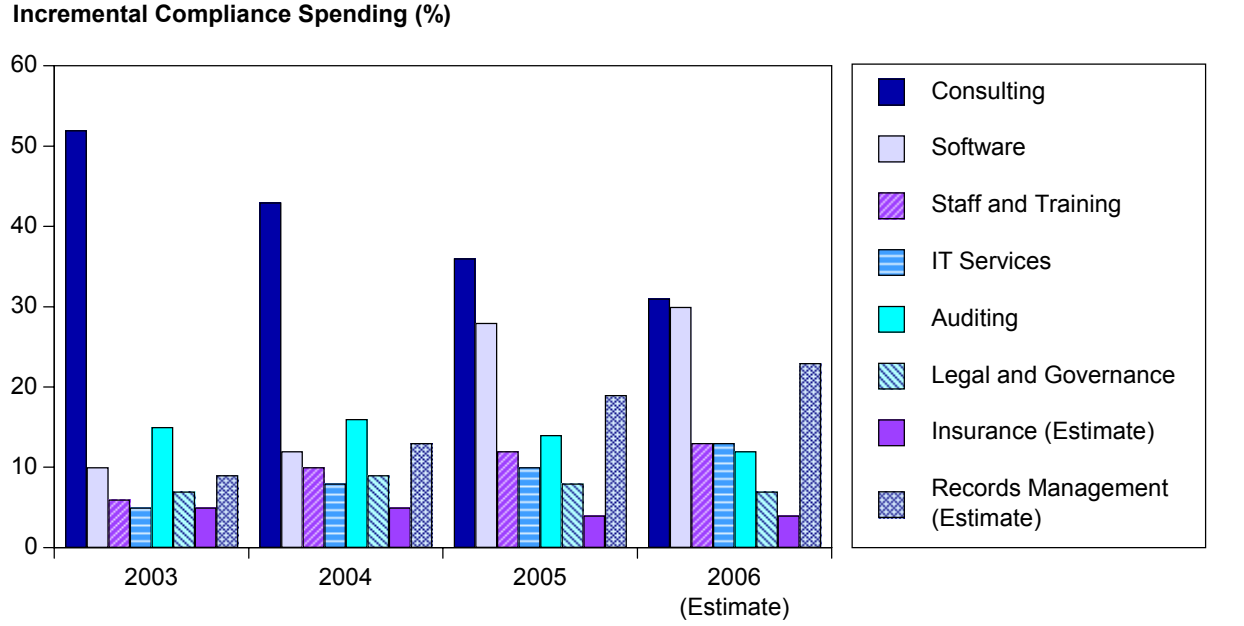
The Gartner TCO methodology assesses IT costs over time. It takes into account all the costs associated with IT investments, including capital investment, license fees, leasing costs, service fees and internal labor costs. It includes direct (budgeted) costs, such as capital hardware and software, labor operations and administrative line items. It also includes indirect (unbudgeted) costs — that is, those associated around end-user operations, peer support, casual and formal learning, self support, application development for personal business use, file and data management, and downtime. The core of the TCO methodology is a chart of accounts that lists the line items in each category and the cost to complete or procure those items (see "Defining Gartner Total Cost of Ownership").

© 2006 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

Awareness of the dynamics of TCO is crucial to managing the cost of compliance. Unfortunately, business and information systems complexities are increasing TCO faster than best practices can be developed to mitigate those costs. Complexity grows with the growing number of compliance requirements. These include legal regulations, such as SOX, HIPAA, environmental laws and Basel II, as well as compliance issues brought about by mergers and acquisitions, supply chain complexity and siloed projects.

Figure 1 gives a breakdown of the elements of compliance costs from 2003 through 2006.

Figure 1. Accounts for a Compliance Cost Model



Note: The Standard & Poor's 500 spent an incremental average of $4 million, and the next-500-largest U.S. companies spent an average of $3 million, on compliance management in 2005.

Source: Gartner (June 2006)

2.2 Role of Best Practices

By examining best practices, companies can optimize the efficiency (ratio of cost to risk) or effectiveness (service level) of the business process. Best practices will provide indicators for operations that are replicable, transferable and adaptable across industries. Best-practice categories include the traditional infrastructure TCO processes, such as change management, operational management, asset administration, technology planning, process management, customer service, and training — all or some of which may impact the cost of compliance. Furthermore, best practices regarding architecture, governance and program management that are relevant to compliance are also included in the overall TCO analysis. These features are discussed further in Section 4.0.

2.3 Assessing Risk

When considering compliance costs, the issues of regulatory compliance require a new factor, risk, to be added to best-practice categories. Many methods for risk analysis are precise but complex. Look for simple methods of risk analysis — such as failure modes and effects analysis

© 2006 Gartner, Inc. and/or its Affiliates. All Rights Reserved.
Gartner

(FMEA) — that will provide a snapshot of where to make qualitative adjustments to your risk investments (see "Gartner's Simple Enterprise Risk Management Framework").

2.3.1 Failure Modes and Effects Analysis

FMEA is a qualitative reasoning approach to risk analysis that focuses on three key elements: severity, probability and detectability.

FMEA's roots are in testing mechanical and electrical hardware systems. However, it has been adapted to support a wide range of industries and applications, from medical patient care to software application development.

As adapted to compliance, the FMEA technique has two major components. The first is that it considers how the failure modes of each system component — that is, noncompliance — can result in the company's overall survivability. Second, it suggests what appropriate safeguards might be in place to overcome noncompliance.

2.3.1.1 Phases or Aspects

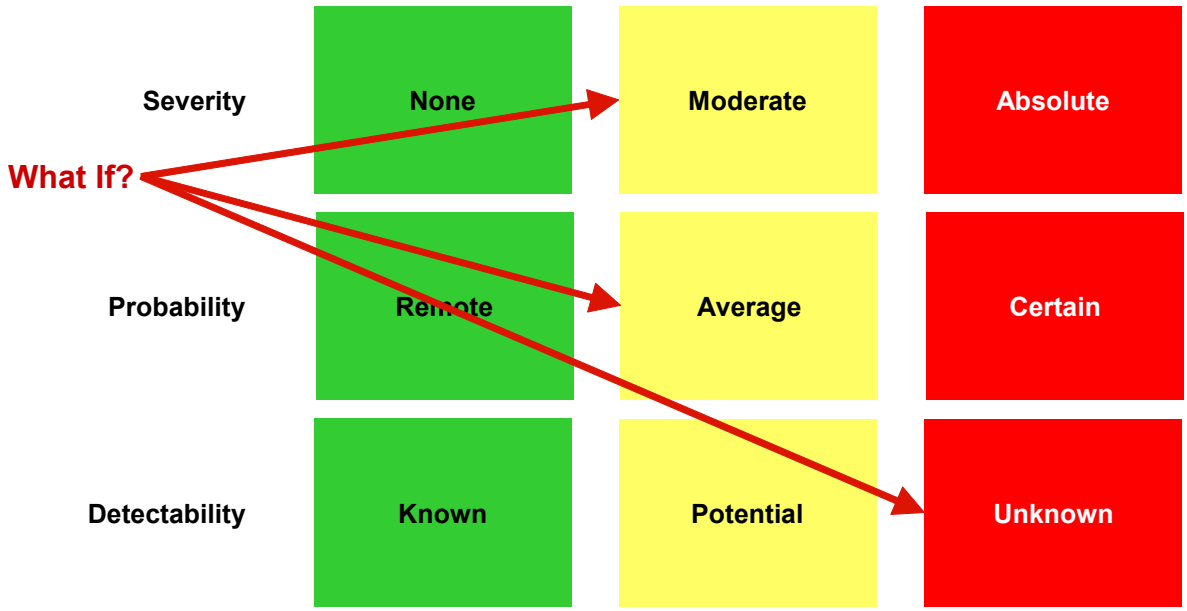
FMEA looks at three key areas and rates each:

- Severity — None to moderate to absolute
- Probability — Remote to average to certain
- Dectability — Known to potential to unknown

In Figure 2, we have a potential case of noncompliance that is average in its probability, with uncertain detectability. However, noncompliance has only a moderate impact on the organization. Looking at this potential noncompliance issue, management must ask itself, "Is this an acceptable level of risk?"

© 2006 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

Figure 2. The Spectrum of Risk: What Is the Worst Credible Outcome?



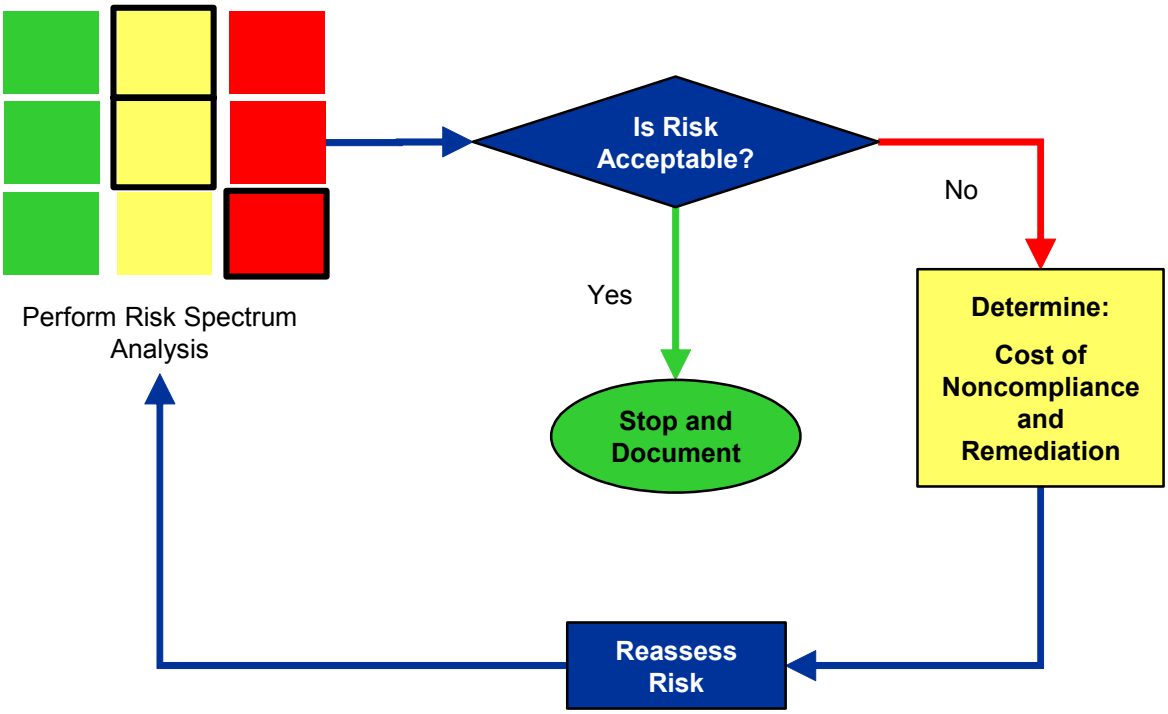
138098-2

Source: Gartner (June 2006)

Figure 3 shows how the FMEA model can be applied to assess compliance risk in an enterprise setting. It provides a framework to explore the appropriate risk response and asks, "What is the most appropriate action, given our tolerance for risk and the severity of the noncompliance?"

© 2006 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

Figure 3. FMEA Approach Applied to Compliance



Source: Gartner (June 2006)

2.4 Seek Additional Value From Compliance Through Aggregation

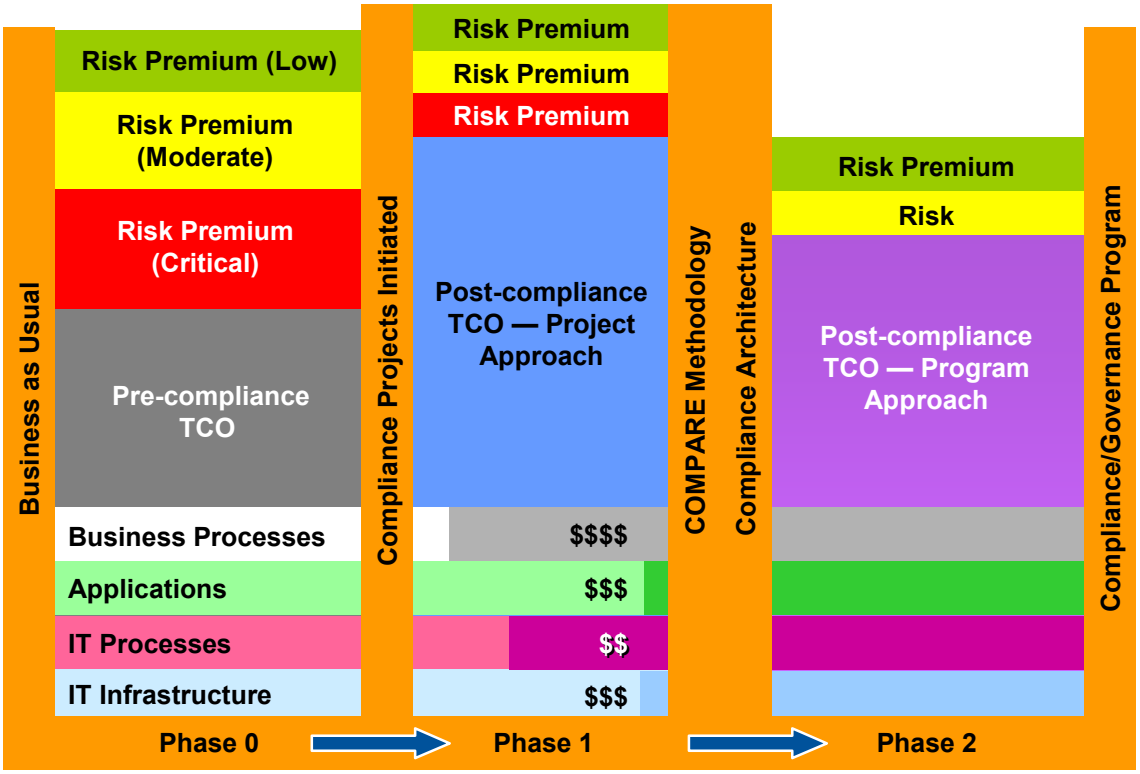
Pre-compliance TCO attempts to capture all the costs of IT investments throughout the IT resource life cycle. Costs are accounted for during planning and acquisition, deployment, management and support, and retirement or replacement. These costs then are annualized to normalize labor and capital costs.

With the introduction of compliance requirements, management must determine the level of compliance desired and required, as well as taking into account the potential risk of noncompliance. The post-compliance TCO is based on the execution of stand-alone compliance projects, and it drives up cost incrementally, primarily because of increased complexity (see Figure 4).

Complexity is a factor that typically increases cost. Complexity can be good if it introduces useful new features and can be tolerated by the business. Good complexity has a positive return on investment in that the new features offer corresponding business benefits. Complexity can be bad if it is caused by redundancy of systems, heterogeneity of infrastructure or features that are unexploited.

© 2006 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

Figure 4. Preparation and Cost of Compliance



138098-4

Note: $$ = least expense, $$$ = moderate expense and $$$$ = most expense.

Source: Gartner (June 2006)

Compliance cost and risk mitigation occur in all layers of IT. For example, the compliance-enabled infrastructure level may require new security measures, new operations procedures, more-robust processing and storage management. Certainly, IT processes for change management, asset management, problem and incident management, documentation, security and auditability will need to be more mature. Applications will need more features to meet control requirements, and business processes will need more checks and balances to be compliance-enabled. A TCO model must address the IT component of each of these layers.

A compliance-enabled architecture will determine how each of these layers works together (or not). The compliance architecture is detailed further on in this document.

The compliance-enabled governance model is the business equivalent of architecture. Governance determines how decisions are made and who makes them. IT governance as a subset of corporate governance will need to have a new awareness and competency in compliance issues.

Figure 4 illustrates the impact of TCO in its pre-compliance state (red) and post-compliance state (green). Note that TCO is applied to IT projects and IT operational processes. In Figure 4, we show the day-to-day operating cost of compliance. The third block (purple) takes into account the risk adjustment that occurs as a function of the controls built into the post-compliance state. One way to express risk as a cost element is to estimate what it would cost to insure against a lack of controls, and we have deducted that insurance cost from the post-compliance TCO. Although this

© 2006 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

chart is for illustrative purposes only, it demonstrates the decision-making capability and impact analysis that a TCO study can provide.

3.0 IT Cost Drivers of Compliance Mitigation

Understanding what drives compliance costs allows you to capitalize on labor and investment, systems integration and standardization. Understanding these drivers also improves manageability.

As the number of compliance projects grows, the cost of meeting those requirements grows substantially faster. Several factors are important in controlling compliance costs: looking for commonality; using existing and new investments; and taking as much complexity out of the system as possible.

Looking at Gartner's formula for calculating the appropriate compliance cost for a single project, we believe:

Compliance_Project = Sum [E*(1+lnC)]

Where:

- **E** is a cost of making some project compliant when its complexity is lowest — that is, C = 1 (and E of different projects could be different).
- **C** is a complexity of a separate project (and complexity of different projects could be different). C varies from 1 to 10.

Cost of a separate compliance project is a function of C, and is not (and should not be) a function of the number of projects (N). Cost of compliance applied to all N projects is a function of N and C.

In tackling multiple compliance projects as a program, we suggest:

Compliance_Program = [Eave*R + Eave*(1-R)*N] * (LN(1+Cave))

Where:

- **Eave** is an average cost of all N projects.
- **R** is a typical percentage of the project budget that is being spent on tools and technology — (1-R) is a percentage of development expenses.
- **LN** is a natural logarithm.
- **Cave** is an average complexity of all N projects.

We begin with the assumption that capital investment in the combined project stays the same as if it were a single project, but the development cost is a linear function of combined projects. To calculate the IT portion of the cost of compliance, you start by looking at the traditional direct (D) and indirect (I) IT costs. As you introduce complexity (C) in meeting compliance, those costs drive up the total of compliance rapidly. At the same time, best practices have the ability to drive out costs, but at a much slower rate. All of this, however, is amplified by the potential risk involved in not meeting or maintaining compliance.

These formulas describe and approximate the general trend that we believe is occurring. They give a good starting point for evaluating cost of compliance, although they could deviate from a

© 2006 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

specific project cost. However, as an approximation of a trend, they are useful, although we have not tested them in a large number of cases.

3.1 Complexity

Infrastructure TCO data shows that as complexity increases incrementally, cost rises increasingly rapidly. When this phenomenon is coupled with a reactive project mentality, the costs will quickly become unmanageable. The same is true with compliance analysis, with the caveat that the compliance issues are already much more complex than infrastructure issues.

Complexity exists in the IT infrastructure and application portfolio and in the business units. The value of good governance, a holistic view of compliance issues, business process simplification, and a consistent technology and business architecture will go a long way toward better management of the total cost of compliance.

To reduce compliance costs, businesses must aggregate their compliance requirements, appoint authoritative leadership, allocate adequate resources and develop a detailed but unpretentious project plan. Compromise on any of these elements, and you will waste money, miss deadlines and increase risks.

3.2 Compliance Effectiveness Related to Cost

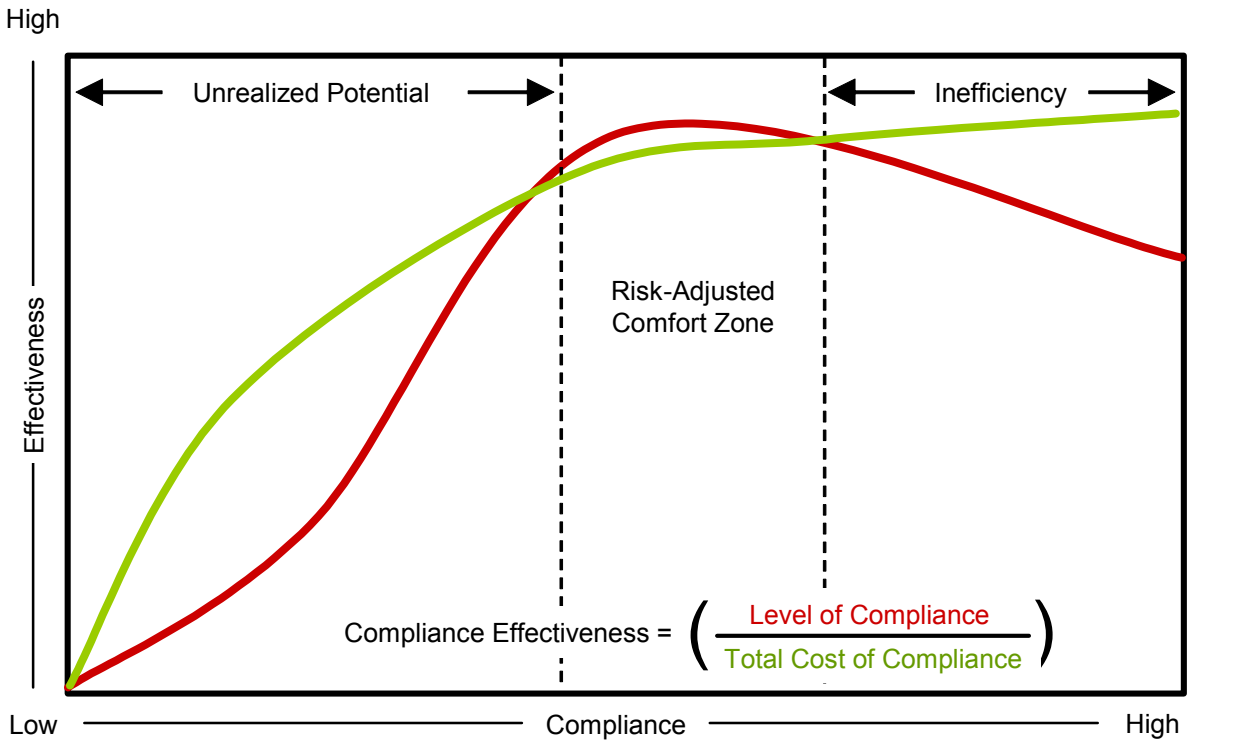
One of the ways to evaluate the effectiveness of a compliance program is by looking at how well it works versus how much is spent to achieve the level of compliance that management deems sufficient.

Based on research by J.M. Juran and F. Gryna in "Quality Planning and Analysis," we can identify three operational zones of compliance (see Figure 5):

- *Unrealized potential* — The compliance infrastructure is capable of cost-effectively delivering existing, and higher, levels of compliance. In this area, the potential exists to cost-effectively reduce compliance risk exposure by increasing the operating level of compliance.
- *Risk-adjusted comfort zone* — The compliance infrastructure is performing close to its maximum effectiveness. The objective is to maintain status quo by monitoring the evolution of costs and potential risk exposures.
- *Inefficiency* — The compliance infrastructure is incapable of cost-effectively delivering the required compliance level. Here, the business must think about reducing how much it is spending on compliance and look at improving its compliance programs.

© 2006 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

Figure 5. Strike an Appropriate Balance Between Effectiveness and Efficiency



Source: IBM Consulting's "Risk and the Economics of Regulatory Compliance" and Gartner (June 2006)

Operating at a level of compliance below that required by management's preferred risk profile jeopardizes shareholder value, reputation and revenue. There is a minimum cost required to achieve a desired level of compliance, but spending more does not necessarily mean a business is more compliant or has reduced its risk.

4.0 Managing the Cost of Compliance

Achieving compliance is merely one aspect of a series of activities that should lead to improved risk management and corporate performance.

Today, many companies focus on meeting, attesting or maintaining regulatory requirements, such as SOX. They may be too consumed with looming deadlines to think about the broader implications of the controls they are putting in place, or how these controls can be automated. However, prudent businesses will allocate resources to maintain compliance even after they have met initial requirements. Unfortunately, previous Gartner research showed that few companies had no annual budget designated to maintaining compliance for something such as SOX. However, as noted earlier in the latest survey data, most organizations now are budgeting IT funds for compliance.

Because compliance requirements are ongoing, all businesses will benefit from replacing a short-term mind-set with a longer-range perspective that embraces an enterprisewide view of compliance. With this approach, they are more likely to respond better to volatility, focus their attention on the risks that matter the most, identify risks they can exploit for competitive advantage and protect shareholder value.

© 2006 Gartner, Inc. and/or its Affiliates. All Rights Reserved.
Gartner

4.1 Measuring Progress Toward Compliance Using COMPARE

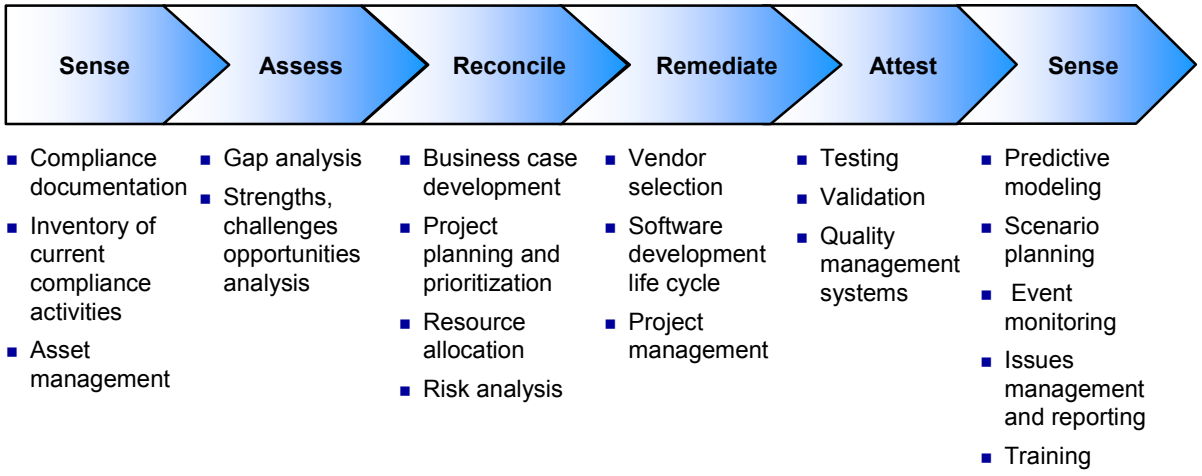
As companies struggled to reach Y2K compliance, they needed to have standardized criteria to assess their progress. At that time, Gartner introduced the Compliance Progress and Readiness (COMPARE) scale. The COMPARE scale defined levels of activity and a standard for measuring Y2K compliance progress and readiness. It also laid out milestones on a scale that could be used to evaluate any organization's process, management and progress toward neutralizing the threat from Y2K failures.

In considering the challenges of compliance, Gartner updated a tool that could map and measure progress. A team of analysts experienced with public policy issues, numerous compliance requirements and IT technology organizations revisited the original COMPARE scale and reprogrammed it to focus and measure compliance activity and progress (see Figure 6).

Gartner's COMPARE cycle is a well-defined, structured process and framework for compliance projects that enables a business to measure its progress toward meeting compliance requirements (see Section 4.2. For a detailed treatment of COMPARE, see "Use Gartner's COMPARE Cycle to Manage Compliance Activities").

COMPARE helps businesses combine multiple compliance requirements. The result is that value begins to emerge from the compliance requirements as business and IT processes, applications and infrastructure are used, and a balance is struck between the cost, risk and benefit of existing and new investments. This improves efficiency and lowers costs in the risk-adjusted TCO environment.

Figure 6. COMPARE and Key Capabilities



Source: Gartner (June 2006)

4.2 Cost-Effective Compliance Requires Effective Governance

Regulatory compliance will involve ongoing efforts on the part of every company. From health and safety legislation to anti-terrorism measures, good regulatory regimes depend on three things:

- *Organizational support* — Compliance officers, compliance committees and internal auditor functions will become essential to doing business. Without the assignment of responsibility, there can be no real compliance.

© 2006 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

- *Process control methodology* — Using open, accessible and peer-reviewed frameworks for risk management and different kinds of control — whether inside or outside the IT organization — will make compliance regimes more transparent to outsiders.
- *Content control* — The only indisputable trail of evidence — either of right practice or wrongdoing — comes through the electronic and paper records that companies keep. Gartner's ongoing experience with all of its clients suggests that 99.9 percent of companies must work on this area of compliance management.

There are, of course, many other aspects of corporate governance, the most important of which is the ethical conduct of business and leadership by example (see "Best Practices on How to Organize for Sustainable Compliance" and "Revised USSC Guidelines Clarify Compliance for Life Sciences").

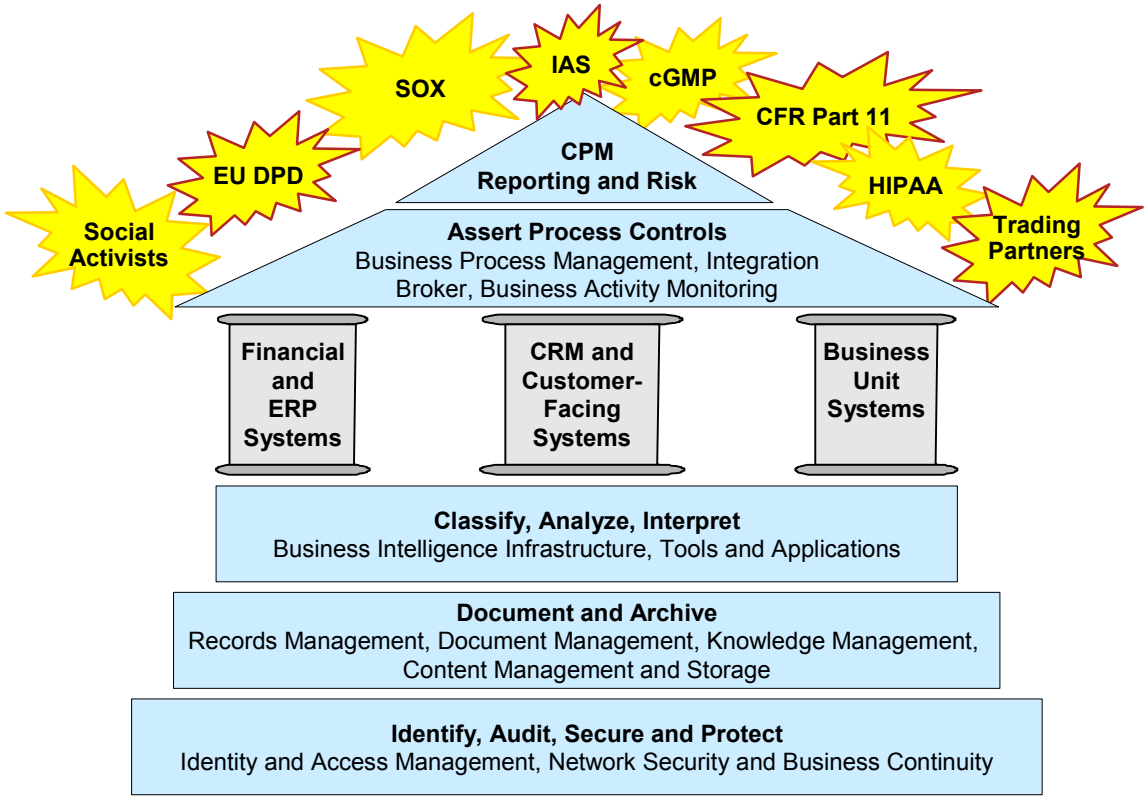
4.3 IT Practices to Manage the Cost of Compliance

Government regulations are unfunded mandates that drain resources from revenue-generating business operations. Vendor hype suggests that implementing a wide variety of technologies is the answer to becoming compliant. However, as with other business issues, it is possible to be good or bad at compliance, regardless of the technology deployed.

A compliance architecture doesn't necessarily require new software investments and does not need to be implemented across the enterprise in a single step. Most companies will find that they already have many of the software tools they need to support compliance. Companies with good security and business continuity planning practices, a document management system and a business process management (BPM) system likely already have the foundation for a compliance architecture (see Figure 7).

© 2006 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

Figure 7. Components of Compliance Architecture



138098-7

CFR = Code of Federal Regulations
cGMP = current Good Manufacturing Practice
CPM = corporate performance management
EU DPD = European Union Data Protection Directive
IAS = International Accounting Standards

Source: Gartner (June 2006)

By expanding and standardizing the use of those systems, adding some business intelligence and perhaps a compliance tool for reporting, you can rapidly deploy a robust compliance architecture. Some of the newer compliance management tools include full document management and business process management capabilities with templates for specific regulations to ease deployment. A survey of internal applications should help you to determine which compliance architecture components you already own.

4.4 Creating a Central Compliance Authority

The compliance program office uses people, processes and technology to help your enterprise operate in an integrated state of control. The program management office for compliance is similar to other program management office structures, controlling:

- Tasks
- Resources
- Progress

© 2006 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

- Expenditure related to ensuring regulatory compliance

Most compliance management offices focus on integrating compliance within daily business operations. This can help the enterprise move from an informal qualitative approach to understanding risk to an approach that is more quantitative and uses objective criteria for determining and managing risk.

The compliance management office can help:

- Define compliance strategy
- Align leadership
- Mobilize trained resources
- Provide a single view of all efforts
- Ensure consistency
- Train and coach on methods
- Prepare for anticipated regulations
- Create tools and templates
- Capitalize best practices
- Create compliance infrastructure

If no compliance management office exists, create one. If it does exist, evaluate its effectiveness, making adjustments to funding, staffing and responsibility, as required.

4.5 Anticipate Future Compliance Requirements

The true business benefits of compliance go beyond improving performance through monitoring and corrective action. When your business has developed forecasting skills that allow it to see "over the horizon," benefits will come in the form of improved corporate performance. One way businesses have developed this broader perspective is to create a function called the public policy "weather bureau."

The weather bureau accesses legal and historical expertise and is charged with the acquisition, assessment and analysis of information about consumer and regulatory trends. The forecasts produce reasonable scenarios for the program management office to evaluate developing policies. The legal outlook must become a primary input to the strategic planning process and to any tactical choice that you make to establish yourself in the marketplace or gain market share (see "A Method for Tracking Life Sciences Public Policy Issues").

5.0 Conclusions

Enterprises often view compliance efforts as unique projects driven by individual regulatory requests. A better approach is to view compliance as a process that improves corporate performance management, and for many organizations, it can lower cost and enhance quality.

SOX is only the latest of many compliance challenges. As we await the next initiative that will demand corporate attention, we must prepare for a regulatory environment that will grow more onerous, not less. Businesses can respond to regulatory compliance by:

© 2006 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

- Taking an ad hoc approach — Addressing requirements as they emerge and treating them as one-time and just-in-time projects
- Being more proactive and designing a comprehensive process aimed at department needs
- Adopting an enterprisewide view that is more strategic and looks further into the future

Each business will need to make a determination of which approach to use based on its risk tolerance and business performance objectives. Nonetheless, ad hoc or departmental approaches to enterprisewide compliance topics will not provide the needed effectiveness. Compliance should embrace enterprisewide processes; also, it should be managed and supported by owners, well-designed systems and appropriate technology.

The real goal of compliance efforts should be to help the company do business better. The revised amendments to the U. S. Sentencing Commission Guidelines that strengthen the criteria for an effective compliance program indicate the importance of these efforts. Companies must demonstrate that they have exercised due diligence in fulfilling the compliance requirements and have established a company culture that "encourages ethical conduct and a commitment to compliance with the law."

6.0 Recommendations

- Companies with frequent, burdensome or complex compliance issues should create a compliance program office to manage all compliance issues from an enterprisewide perspective.
- Combine compliance requirements and build synergistic solutions. The effort saves time and money as well as establishes a framework for responding to future requirements.
- Set the compliance bar at the level that matches the company's risk profile.
- Monitor the total cost of compliance relative to effectiveness. Higher expenditure will not necessarily mean a higher level of compliance or reduction of risk.
- Understand, categorize and communicate the risks of noncompliance. Agree on the company's preferred risk profile.
- Implement a risk-driven compliance approach that will work for any new mandates that come along and will improve reporting capabilities.
- Create a weather bureau to watch for changes in governance and compliance requirements.
- Create an explicit link between compliance, performance management and value.
- Manage compliance as a program, not a project. (Regulatory compliance must be continuous.)
- Effective compliance requires organizational support, process control methodology and content control.
- To control compliance costs, look for commonality in compliance requirements, use an investment approach for budgeting, and take complexity out of the system whenever possible.

© 2006 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

RECOMMENDED READING

"Understanding the Components of Compliance"

"A Method for Tracking Life Sciences Public Policy Issues"

"Best Practices on How to Organize for Sustainable Compliance"

"Revised USSC Guidelines Clarify Compliance for Life Sciences"

"Use Gartner's COMPARE Cycle to Manage Compliance Activities"

"Defining Gartner Total Cost of Ownership"

"The IT Executive's Best Practice Guide to Sarbanes-Oxley"

"Examine Sarbanes-Oxley Section 404 Weaknesses and Use IT as Your Solution"

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

© 2006 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

Gartner