



Debunking the Top 5 Myths of Compliance

Myth #1: Compliance Initiatives Don't Align With Business Objectives (Compliance Initiatives Are Bad For Business)

One of the major complaints about the flurry of recent regulations to arise over the last decade is the financial impact to businesses from meeting compliance objectives. These costs, combined with a strong increase in the size of penalties associated with regulations, lead many people to question whether the ultimate impact of the regulation does more harm than good.

Underlying these complaints is the general feeling that compliance initiatives are antithetical to business objectives, and that the tasks required to meet those initiatives are a hindrance to efficient business practices. In the current "do more with less" high efficiency business environment, compliance is often seen as unnecessary overhead which does little to bolster the success of an organization.

This line of thought simply isn't true, and in fact, many of the compliance initiatives that have been the target of recent attention actually underscore basic operating tenets that are the foundations of good business. A cursory review of recent regulations reveals that five of these tenets seem to appear with regularity in compliance directives: Accountability, Integrity, Custodianship, Risk Management, and Standardization. On closer examination, these basic concepts prove to be good for both business and compliance initiatives.

Accountability

Good for business: Accountability is a term that is bantered around frequently in our post-Enron environment. It speaks to the concept that each member of an organization is responsible for the completion of specific tasks and objectives. Each person is answerable not only for the completion of his or her tasks, but also for the thoroughness and accuracy with which the tasks are performed.

Compliance directives focus on assuring accountability in the most critical aspects of business operations. Emphasis is placed on sign-off and record-keeping controls that demonstrate with absolute certainty the identity of the person responsible for each function. Moreover, it is rarely enough to show that a sole individual has been held accountable for the task. Frequently, one or more levels of management must be able to prove that they reviewed the completed work and that it meets appropriate standards.

Debunking the Top 5 Myths of Compliance

This accountability is the underlying impetus of the Sarbanes-Oxley Act, which requires the highest levels of an organization to attest to the accuracy of financial statements. This level of attestation holds executives in an organization personally accountable for the work presumably done by their subordinates. Privacy acts such as HIPAA and Gramm-Leach-Bliley also seek to enforce this accountability.

Good for compliance: A close examination of the basic functions of organizational structure reinforces this concept of nested accountabilities. Modern businesses, and most other modern organizations, are hierarchical and departmental in nature because it's the structure that most effectively fosters role specialization and allows organizational members to build expertise in key areas. If an organization did not have this division of responsibilities, every member would be responsible for performing every activity, no specialized talents would emerge, and suboptimal results would most likely follow.

Integrity

Good for business: Integrity has become a cliché in the mission statements of corporations today. The concept of corporate integrity is often a broad statement of the corporation's commitment to business ethics. Yet integrity in the compliance context is more a component of the trustworthiness of statements made by and about the business.

A pillar of the corporation's social contract is its responsibility to accurately report the status of the corporation, its operations, its assets, and its financial stature. Recently, this contract has been extended to include statements about a corporation's protection of key assets. A company who states that their customers can depend on the security of a website is expected to have provided some assurance to maintain that security.

Debunking the Top 5 Myths of Compliance

So integrity has been extended to mean the reliability of statements made not only about the company's finances, but also about its operations. There are two questions frequently asked to validate this reliability:

1. Are the persons making those statements truthfully representing the company's posture?
2. Did the systems that produced the data used to support those statements generate accurate information?

These questions are being asked now not only by the public, but also by investigators, auditors and regulators responsible for corporate oversight. At first glance, the occurrence of a dishonest executive and a corrupted computer system seem to be unrelated business problems. In fact, they are inextricably linked through their common remedy: controls.

Good for compliance: The heart of regulations designed to enforce the integrity of business statements and operations are the controls that businesses use to establish and protect the credibility of those statements. Frameworks such as COSO are cited by regulatory bodies because they define controls that are most appropriate for business objectives. These regulations are underscoring the importance of integrity because of a well-publicized recent history of corporations failing to provide that integrity on their own.

Custodianship

Good for business: One of the underlying principles of today's corporations is executive managers acting in the best interest of shareholders. Simply put, corporate leaders manage assets which they do not necessarily own. This custodianship is an expectation of all corporate directors. The idea that the people in the corporation must faithfully manage the assets for which they are responsible is an idea as old as the corporation itself.

Traditionally, the directors of a corporation had the most custodial obligation toward protecting the financial value of the company and its ability to operate profitably. Over the last century, we have seen corporate management also held accountable for some of the softer assets of the company, such as company reputation and customer loyalty.

Debunking the Top 5 Myths of Compliance

Recently, customer demands as well as regulations have broadened corporate responsibility to include custodianship for assets not even owned by the corporation. The most obvious of these responsibilities is the protection of customer data. Fifteen years ago, if you pointed to a company's customer database and asked the directors of the company "Who owns this data?" the answer would have been that the company owned the data. For all practical purposes, they did.

Good for compliance: Recent breaches of customer data that resulted in identity theft have caused companies to reconsider the relationship to that data. Privacy regulations now make it clear that the data belongs to the customer, and that the corporation is merely a custodian of the data. The company, therefore, has a greater responsibility to protect that data. No longer can the company consider its own needs when deciding appropriate controls around customer data. The obligation of the company to protect that data on behalf of the customer far outweighs the company's obligation to itself.

The expansion of custodianship to include records and information for which the company as a whole must manage, but does not own, has reinforced one of the primary constructs of the publicly owned company.

Risk Management

In business, the term "Risk Management" can take on many different connotations in many different contexts. At its core, it describes a process of making decisions based on a cost-benefit analysis.

Good for business: When this analysis of costs and benefits is applied to the protection of company assets, the expectation is that there should be an increase in the amount of risk that is mitigated with every dollar of control that is implemented. This sort of ROI equation is a basic component of asset protection. No matter what kind of business you are in, you never want to implement \$100 of security to protect a \$1 asset.

However, if a company fails to accurately assess business risks and spend the appropriate resources to mitigate those risks, the company puts its business in jeopardy. Many companies have failed in the past to understand the way that true risk is evaluated. Modern organizations are starting to gain enlightenment as to the real risk value.

Debunking the Top 5 Myths of Compliance

A bank that which keeps \$1 million of its customers' money in a vault may state that the maximum they would want to spend to protect that vault is \$1 million. In practice, they would spend far less than that and insure the money to mitigate the remaining risk. But what is the real loss to the bank if the vault is breached and the money is stolen? Once the insurance company pays out to replace the \$1 million, the bank still has additional losses. Decreased customer confidence, bad publicity, loss of stock value, and rising future insurance costs are all hidden risks that the bank must consider.

Good for compliance: Many regulations such as FISMA and HIPAA now require organizations to perform a true risk assessment when evaluating the strength of their controls. Businesses must now look at the bigger picture to determine the real loss expectancy. Business plans for disaster recovery use these formulas to help capture hidden costs such as the cost of temporary operations until normal operations resume. Privacy regulations, for example, may require businesses to absorb the cost of credit protection services for customers whose information was stolen.

The changes in regulations around how businesses mitigate risk are causing companies to reconsider their risk models in all areas of operations. As businesses are shown how to better evaluate their total risk exposure, they are empowered to make better risk management decisions.

Standardization

Another byproduct of recent regulatory changes is that businesses are looking for ways to standardize their operations to meet these objectives. While standardization has long been the mantra of companies looking to be more competitive through operational efficiency, it is also gaining popularity as a solution to compliance and risk challenges.

Good for business: As companies look to streamline operations, standardization has become a process not only for reducing costs, but also for ensuring repeatability of processes and consistency of operations. Since the time of Henry Ford, companies have embraced the idea that good processes, when repeated, produce consistent results. Recent movements in information technology have looked to standardization to ensure economies of scale. One mechanism for this

Debunking the Top 5 Myths of Compliance

efficiency has been standardizing to allow many disparate systems to be consolidated. Data center consolidations, virtual server consolidations, even management utility consolidations have proven not only cost-effective, but also highly reproducible for disaster recovery purposes.

Good for compliance: It is no surprise, then, that regulators look to consistent, standardized processes and controls as a way to ensure not only operational efficiency, but also process integrity. Standards such as the Center for Internet Security (CIS) Benchmarks are laying the groundwork for companies to introduce common sets of consistent, effective controls throughout IT environments. National Institute of Standards and Technology (NIST) also issues recommendations on standard system configurations.

Many businesses are recognizing that the standardization of processes, systems, and configurations has a significant upside, not only on their operational efficiency, but also on their compliance posture.

While these five components, Accountability, Integrity, Custodianship, Risk Management, and Standardization may seem like basic tenets to the daily operation of the modern corporation, it is important to remember that they are also foundational elements in many of the requirements of our current regulatory atmosphere. Far from being antagonists to the smooth operations of a company, these agents of regulatory change are also cornerstones of business operations.

Myth #2: Compliance Can Be Solved with a Project

One of the major fallacies of addressing new compliance regulations is the idea that companies can handle compliance requirements through a project. Employees who are only now being involved in compliance remediation are frequently overheard to refer to "that Sarbanes (Oxley) project" or "the HIPAA project." Even in public sector agencies, there is often planning to ramp up resources for "the annual FISMA project."

In truth, compliance is frequently an objective which dwarfs other projects in the organization. An April 2005 report, prepared by the Charles Rivers Associates on behalf of the Big Four accounting firms, was delivered to the SEC to help quantify the costs of Sarbanes-Oxley compliance. The report, titled "Sarbanes-Oxley Section 404, Costs and Remediation of Deficiencies," sampled 90 of the Fortune 1000 companies and found the average expenditures for compliance averaged \$7.8 million per company, an average of one-tenth of one percent of each company's revenues.

The myth of addressing compliance in a project is not in the handling of the workload management, but in the fundamental definition of a project. Project managers frequently like to point out that a project must have a starting point and an ending point. Although a project may be repeatable, it reflects a unique process or series of events that is not integrated into daily operations.

This approach to addressing compliance initiatives stems from companies' successes managing what they view to be similar initiatives in the same manner. The massive IT validations of Y2K were a painful enough part of the recent past that they are fresh in the minds of many corporate managers. Corporate leaders still equate many large IT validation projects to the Y2K experience. Similarly, many companies shored up their disaster recovery efforts after September 11th. These events were viewed as one-time objectives to be completed and set aside in favor of new business goals.

Businesses that give proper treatment to Business Continuity Planning and Disaster Recovery planning have now prioritized that planning as part of their regular operations. When new systems, processes, or even business acquisitions are brought in to business, their impact on BCP and DR is carefully weighed during the earliest stages of the integration projects.

Debunking the Top 5 Myths of Compliance

Organizations must take this approach when dealing with regulatory compliance. Instead of being a one-time project, compliance must be integrated into core business requirements and become a component of all other projects. As with Disaster Recovery initiatives, businesses that make compliance a cornerstone of their overall strategy will be most successful at meeting compliance requirements year after year. Frequent reviews of an organization's security and compliance posture will help assure continued compliance.

Another reason to reject the project approach to compliance is the fluid compliance landscape. As new regulations are introduced and existing regulations enter additional phases or are expanded, corporations are left feeling that they are trying to hit a moving target. Many compliance regulations are phased in to lessen impact to businesses. However, if those phases are not managed correctly, a compliance project can be prone to perpetual "scope creep," with all of the associated resource drains and cost overruns that moving scopes create.

So if not a project, what is the solution to compliance management? The simple answer is a painful one: a paradigm shift to a culture of corporate compliance. Compliance must be integrated into project and business planning methodologies. Each new initiative must be evaluated for its potential impact on compliance requirements. Existing business processes must be reevaluated for appropriate controls that provide the asset protections regulations require.

Addressing the changing atmosphere of compliance requirements is easily handled by a similar paradigm shift. Rather than addressing each compliance requirement as it is announced, organizations can opt to adopt the risk assessment and remediation model that has been the foundation of good information security practices for years. Because the ultimate goal of every security compliance requirement is focused on the protection of assets from risk, compliance objectives may change, but fundamental methodologies do not change. Building effective information security programs into all aspects of business operations will address most compliance requirements. By understanding the value of assets and taking steps to adequately protect them, organizations will find themselves meeting compliance objects for financial integrity, privacy, systems security, and whatever the next big compliance hot button might be.

Additionally, an information security compliance program can be established as a fixed, manageable cost of daily operations. The costs and resources required can be managed according to organizational priorities, not deadlines imposed by third parties.

Companies that adopt this model will begin to evolve into a new level of organizational maturity. Predictably, we will begin to see the evolution of zero-day compliant organizations. These organizations will have such integrated processes around the protection of business assets that new regulations will require little or no operational changes to integrate into company processes. The companies who completely understand how to manage an effective information security compliance program will outpace new regulations with their own protection initiatives.

Myth #3: Compliance Is nn IT Problem/ Compliance Is n Finance Department Problem/ Compliance Is n Legal Department Problem—Compliance Is "Their" Problem

One of the side effects of corporate efficiency initiatives is that departments within companies have learned to compete for resources, funding, and staffing to complete their operational objectives. These groups are often unwilling to surrender precious resources to initiatives that do not support their specific objectives. Compliance initiatives are not typically seen as supporting anyone's objectives, and thus are not easily assigned resources or capital.

Add to this struggle the ever-present disconnect between operations groups and support groups such as Information Technology and Legal, and full-blown turf wars ensue. Regulatory compliance is frequently assigned from department to department, looking for the best fit. Business units see anything dealing with computers as an IT problem. IT sees the regulation as a legal problem. Legal sees any operational requirement as a business unit problem.

The reason that these issues don't seem to fit in any one department is that they are higher-level business concerns, and affect all departments. Consider this statement:

There are no security requirements. There are no audit requirements. There are no compliance requirements. There are only business requirements. Can a corporation make a business decision not to comply with a regulation? Yes.

In some situations, corporations have made the business decision that the cost to comply with a regulation overshadows any penalties or fines for non-compliance. As long as the company can

Debunking the Top 5 Myths of Compliance

act with free will to choose compliance, compliance with regulatory requirements becomes a business decision. Since that decision affects the viability of the whole company, everyone has a stake in seeing compliance come to fruition.

One of the toughest obstacles to overcome in making changes is natural organizational inertia and resistance to change. Successful Information Security professionals have found that these changes cannot happen without total business unit buy-in. Controls which are dictated to a business unit won't be followed until the business unit employees understand, accept, and agree to promote those controls into operations.

In order to successfully gain business unit buy-in, IT and security departments need to be able to understand each other's problems. IT must understand the hard and soft costs associated with changing a long-standing process, as well as the need to maintain operations. Business units must understand the challenges that IT faces trying to keep systems running, up-to-date, and protected. This understanding will promote an atmosphere in which all parties are able to attack both the business and technical issues surrounding compliance.

Myth #4: Information Security Compliance Is About Protecting Computers

Information technology has executed upon business an evolution that rivals or even exceeds the metamorphosis of the industrial revolution. The uniqueness of computers as a business tool is in their amazing ability to continue to transform our lives, our commerce, and our society. It should come as no surprise, then, that when business begins to feel the growing pains of those transformations, it looks to the computer itself as both the root cause and the cure of its problems.

As illustrated earlier, the problems being addressed by compliance legislation are inherent struggles of business, and although they are amplified by the information revolution, they are not unique to it. It is simplistic, then to look to the computer as the source of all modern business security ills.

In addressing the requirements of compliance directives, organizations must look beyond just computers to three different components of their operations: their systems, their people, and their processes.

The United States Federal Information Security Management Act of 2002 (FISMA) is notable for its detailed and practical approach to information security compliance. FISMA addresses computational resources not as individual machines, networks, or applications, but as systems.

Debunking the Top 5 Myths of Compliance

A system is a collection of computers, networks, applications, and other computational components that work together to provide a specific business function, or related business functions. The system is an artificial construct which is frequently hard to define, but taken holistically, appropriately maps to the business function that these resources support.

What, then, is the requirement of regulations which mandate the management of systems? It is the requirement to ensure that resources on that system remain available to the business, that the system maintains the appropriate level of confidentiality required for those resources, and that the system continues to operate at a high level of computational integrity. These three criteria are focused on ensuring that the system continues to service operational needs as it was intended, without compromising other aspects of operations.

The problem with systems is that they frequently grow so large and encompass so many technologies, that aspects of the system can be difficult to predict. Changes made to one component of a system may have repercussion in another component which may go unnoticed for some time. When those changes are affected as an attempt to circumvent, disrupt, or modify the normal operations of the system, it can be difficult to diagnose, isolate, and correct those changes.

One of the earliest concepts in information security was the idea of the Trusted Computing Base. A trusted computing base was a system which was so well managed that the computational integrity of the system was always 100%. With any given operation, input, or change, the system's response or output was easily predicted. While often seen as a theoretical ideal, the trusted computing base is also an important model for practical operations. The idea behind regulatory governance is that organizations should manage systems to this model. This modeling promotes operational efficiency as well as system security.

How then, can this model be realistically employed? By instituting a process of change management, monitoring, and controls that treat computational systems holistically. The current focus of managing individual components and of securing computers must be abandoned in

Debunking the Top 5 Myths of Compliance

favor of the understanding that this model is more comprehensive and more attentive to the needs of business operations. While this theoretical model may never be attained, it can provide business with a lighthouse toward which they can steer their systems management efforts.

Significant emphasis is often placed on hiring the right people to begin with. The integrity of persons working with key business data must be assured. In the past, conducting employee background checks was sufficient to ensure employee integrity. While vetting employees is still an important control, changing ethics environments and business regulations now make appropriate business actions less obvious to many employees. Employee training has thus become an important part of many organizations' operational plans. This training should focus not only on the appropriate content for regulatory compliance, but also the company's policies and practices for conducting operations, including operating computing devices. Policies regarding the use of email, instant messaging, and even removable storage devices are now paramount in ensuring the organization's compliance posture.

This training must focus not only on relating appropriate conduct, but also on gaining employee buy-in and commitment to following these policies and procedures. Asking employees to sign acknowledgment forms stating their understanding of company procedures and committing to conducting business with a high degree of integrity is now commonplace.

In order to set the proper tone for employees to abide by changing regulatory rules, companies must define operating processes that make it easy for employees to understand and follow those rules. Operating processes are commonly instituted to provide consistency and efficiency in the conduct of an organization's business. These processes establish expectations for employees, set control points for detecting non-compliant actions, and provide for corrective steps to restore operations to compliance. It is this level of consistency that auditors look for in judging an organization's ability to not only establish, but maintain compliant operations.

The additional benefit to organizations in the institution of processes is that it raises the maturity level of organizations. Organizations with a well-defined process find that analysis of operational procedures can be more comprehensive. Defined, documented procedures make it easier to identify potential failure points, the controls in place to mitigate those failures, and the strength of those controls. Testing the controls for effectiveness then becomes an easily facilitated task. Ultimately, this natural flow of failures, controls, and testing is the critical information that organizations must present in order to meet their objectives of demonstrating compliance.

Myth #5: One Product Can Do It All

It should be obvious by now that the scope of regulatory compliance incorporates a multitude of business activities, from technology management, to operational practices, to processes and controls. It is interesting to note, therefore, the number of companies that claim to be able to provide comprehensive coverage for compliance concerns. On closer examination, technology products tend to focus on single aspects of compliance, such as managing user provisioning, patching system vulnerabilities or protecting against viruses and malware.

The very scope of regulatory compliance objectives demonstrates that no one software application, suite, or company can solve the complete compliance puzzle. Companies that claim to be comprehensive in their solutions frequently wallow in their own mediocrity, or more dangerously, underestimate the compliance issues that their customers face.

Where then, does software play a role in managing compliance? How can an application solve a problem for a business? The answer to both of these questions lie in understanding that software can only help manage the problem. Software must be a tool in an organizational strategy that emphasizes the importance of meeting compliance objectives.

Therefore, in looking for management answers to any business problem, we look for tools that contain costs, increase efficiency, and meet our business needs.

One of the areas of compliance that has been greatly debated is the cost of implementing controls that meet compliance requirements. Many organizations have voiced objections about the overhead of managing so many disparate business functions to a single standard. These concerns are valid. The modern Information Technology environment is a heterogeneous combination of applications, systems, and networks that support myriad business functions. It takes a sizable, skilled staff just to maintain the operations of this collection of machines. All too frequently, the responsibilities for constantly checking, correcting, and validating security and compliance controls falls to a resource—constricted staff who are already overcommitted to other tasks.

It is this challenge of monitoring, correcting, and reporting the status of dozens of security controls across thousands of IT assets that sets Symantec products apart. The ability to quickly and easily report on the status of a critical control across different sites and even different platforms distinguishes Symantec as a leader in compliance objective management. The efficiencies and cost savings that can be realized by allowing one person to easily generate a single report to gather the same data that would take an army of auditors weeks to generate are truly significant.

Debunking the Top 5 Myths of Compliance

Additionally, to demonstrate the consistency of its practices, an organization must show that it regularly validates the effectiveness of its controls. Effective compliance measurement tools automate validation tasks to schedule systems checks with little or no human intervention.

Symantec's solutions not only automate reporting, but also deliver trend reports that demonstrate how your compliance configuration changes over time.

It is this challenge of monitoring, correcting, and reporting the status of dozens of security controls across thousands of IT assets that sets Symantec products apart. The ability to quickly and easily report on the status of a critical control across different sites and even different platforms distinguishes Symantec as a leader in compliance objective management. The efficiencies and cost savings that can be realized by allowing one person to easily generate a single report to gather the same data that would take an army of auditors weeks to generate are truly significant.

Additionally, to demonstrate the consistency of its practices, an organization must show that it regularly validates the effectiveness of its controls. Effective compliance measurement tools automate validation tasks to schedule systems checks with little or no human intervention. Symantec's solutions not only automate reporting, but also deliver trend reports that demonstrate how your compliance configuration changes over time.

The real value of Symantec's product suite is that it does not act alone. Rather than just a collection of vendor-supplied reports, Symantec products rely on years of experience partnering with businesses, technology groups, and auditors to ensure that their solutions dovetail into existing compliance management frameworks. Symantec's products give organizations the power to build compliance implementations around their own self-defined objectives. Symantec's products also allow a company to interpret high-level guidance such as COBIT and ISO 17799 into concrete, actionable objectives that demonstrate the organization's commitment to meeting compliance objectives.

In fact, Symantec's products demonstrate end-to-end life cycle management for compliance objectives. Businesses are able to manage their systems with a cost-effective solution that allows them to accomplish more than could ever be done before. Based on the define-control-improve life cycle recommended by audit authorities, the Symantec approach allows businesses to see their compliance objectives through to completion. This continuous improvement process allows Symantec customers to demonstrate efficient, effective, compliance management practices.

Debunking the Top 5 Myths of Compliance

And while it is true that no one software product or company can do it all when it comes to meeting compliance objectives, Symantec focuses on the most daunting and inefficient part of compliance management: implementation. Symantec allows companies to just get it done.

Getting Started With Symantec

Regardless of where your organization may find itself on the compliance continuum, or at what stage you may be in the compliance challenge process, Symantec can help. For those facing immediate or imminent compliance audits, Symantec software and professional services provide solutions that can be implemented in a matter of days or weeks versus months. For those who may have completed an initial compliance audit process, Symantec can help to substantially reduce the costs of maintaining and demonstrating compliance on a continuous basis.

About Symantec

Symantec is the world leader in information security providing a broad range of software, appliances and services designed to help individuals, small and mid-sized businesses, and large enterprises secure and manage their IT infrastructure.

Symantec's Norton™ brand of products is the worldwide leader in consumer security and problem-solving solutions providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information.

Headquartered in Cupertino, California, Symantec has operations in 40 countries.

More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745-6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517-8000
1 (800) 721-3934
www.symantec.com

Copyright © 2006 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
01/06

10527718