Building a Culture of Compliance™

Charles H. Le Grand, CHL Global Associates
Sponsored by IBS America, Inc.*
http://www.ibs-us.com

*IBS America, Inc. has been a leading provider of compliance management solutions since 1994.

Overview

This report is about understanding compliance and compliance management adequately to ensure that your organization has the business processes and tools in place to transform compliance from a burden to a benefit. It describes a Culture of Compliance as an integral part of the organization's ethics and describes the elements of compliance that are common throughout the organization. It also suggests a plan to manage and coordinate the common elements of compliance so they can produce efficiencies, maintain consistency, improve reliability and assurance, and result in increased stakeholder confidence. Finally, it identifies the key elements of a system to coordinate compliance management, and provides an Executive Checklist to help assess your organization's Culture of Compliance.

What Is Compliance?

Anyone working in the drug industry is intimately familiar with compliance, but here is a broad definition of the term. Compliance is the act of following the rules. While these rules are often external requirements, and they are many and varied, compliance also involves following the organization's internal rules, policies, and procedures, and acting in accordance with ethical practices. Compliance Management, in contrast, is the means by which organizations can assure compliance in accordance with the rules, regulations, laws, and other requirements to which the organization is subject. Compliance Management involves oversight, assessment, reporting, educating, and noting needs for remediation, while the element of "assurance" comes from reliable evidence of compliance.

Compliance is frequently misunderstood. While recent press attention has focused on the compliance mandates related to Sarbanes-Oxley Act (SOx) requirements, organizations in a wide variety of industries have learned that compliance management is a complex responsibility requiring measurement and reporting against a dynamic and seemingly endless array of rules, agreements, standards, regulations, and legislation. Each area of compliance comes with its own requirements, and in many cases requires extensive knowledge of esoteric technical subject matter and a detailed database for the elements of compliance requirements, measurement, and reporting. In many organizations, compliance management has developed and remained as a series of silos – each meets its own needs but they are not coordinated across organizational levels. This tendency to "silo" often results in duplication of planning effort, redundant reporting systems, misplaced priorities and can waste the scarcest resource in business: management attention.

Compliance –
The list continues to grow

- Quality Management
- Environmental
- Health and Safety
- Industry
  - Chemical
  - Banking
  - Automotive
  - Pharmaceutical
  - Energy
  - Manufacturing
- Employment Opportunity
- Privacy
- Ethics
- Security
- Risk Management
- Financial Processing and Reporting

The silo approach to compliance management has occurred because the organization either realized the advantages of compliance, as in the case of quality management, and/or faced external requirements to comply with specific requirements such as health and safety, environmental responsibility, and industry regulations. While doing so, the organization did not perceive the common elements of compliance management and did not take steps to coordinate different compliance management activities.

An important distinction must be made between Compliance Management and compliance itself because there are two types of compliance activities to improve readability:

- those done for good business reasons regardless of regulations
- those done only because of regulations

Many organizations only refer to activities required by regulations as compliance, but Compliance Management must encompass the assessment, monitoring and control of activities in BOTH categories.

As businesses have become more complex and the need to address competitive pressures and satisfy stakeholder requirements has expanded, compliance management has evolved into a strategic element of business operations impacting everything from corporate governance to comprehensive risk management.

A Culture of Compliance

Best-of-breed organizations understand the advantages of clearly defining, communicating, measuring, and reporting strategic objectives. When results deviate from plans, measurement and analysis provide the information needed to manage corrections, improve prevention and detection, and provide for innovation in returning to the plan or pursuing new ideas and opportunities.

To successfully elevate compliance management to a strategic advantage, compliance must be embedded in a firm's culture – part of the core business model. "All firms have a culture with respect to compliance that may vary. The overall culture within which compliance operates can serve to foster and enhance compliance efforts, or, at its worst, it can impede or render compliance efforts meaningless."[1]

Attributes of a Culture of Compliance

A positive Culture of Compliance includes strategic vision and relates to larger strategic goals. It is:

- established by top management
- characterized by senior management example
- embedded in activities such as education
- reinforced by incentive systems
- given force through the treatment of transgressors
- integral to information systems and their use and management
- inseparable from the organization's structure, processes, and management style

A positive Culture of Compliance also:

- encompasses enterprise risk management
- addresses the risks that arise in each strategic area
- establishes control points for the risk elements
- ensures controls are well documented for internal and external purposes
- identifies the specific people responsible for managing each compliance element

Without a commitment to compliance, even the best policies and procedures will be useless.

Clearly Communicated Vision and Objectives

Clearly defined strategic vision and objectives are central to effective management, and must be consistently communicated across all areas and level of the organization. Measurement and reporting are essential to confirm objectives are consistently met and ensure they will continue to be met. Successful compliance management is also continuous and sustainable throughout an organization and its activities.

"Built-in, not added on."

It is not sufficient to simply publish policies and provide them to employees – they may not read them.

Policy compliance must be integral to management practices and pervasive in all processes and reporting.

The Three C's of Compliance

Compliance has, as its basis, three essential and continuous elements:

- Communication
- Confirmation
- Correction

[1] Lori A. Richards, Director, Office of Compliance Inspections and Examinations, U.S. Securities and Exchange Commission, in a speech for the Spring Compliance Conference; National Regulatory Services, Tucson, AZ, April 23, 2003 – see http://www.sec.gov/news/speech/spch042303lar.htm.

The Three C's of Compliance relate to internal objectives and response to external requirements. They establish the tone for how each individual employee regards his or her role in compliance. They allow compliance to be a benefit rather than a burden. With communication, confirmation, and correction at the center of the organization's compliance focus, it can then radiate outward via compliance management (policies, procedures, processes, systems, and strategies) for all areas of compliance facing the organization from the market, industry, and regulations.

Communication

Compliance communication begins at the top. An organization's leaders establish its ethical tone and state its values, then communicate these clearly to all personnel, ensuring that constant reminders are in place and are integral to such actions as compensation, rewards, promotions, etc. Employees must receive a clear and consistent message:

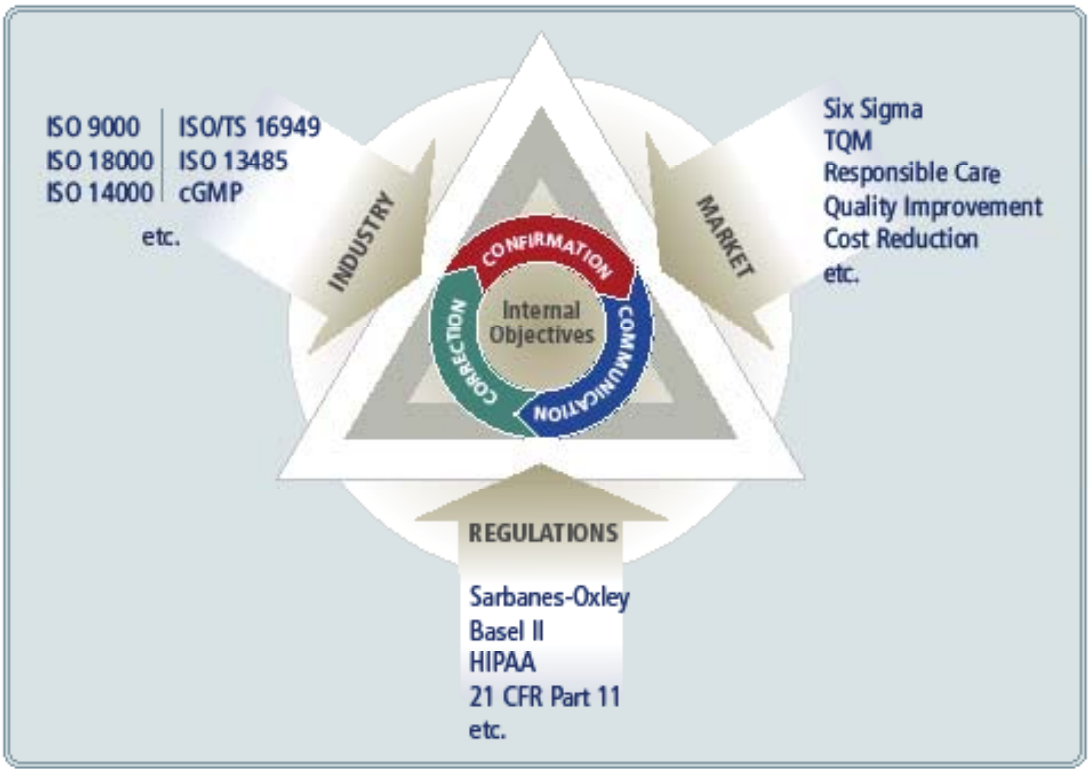
> *This organization meets its obligations. We comply with external requirements and provide sound evidence of compliance. Our customers and business partners know they can rely on us. We not only produce the required reports of compliance, we use them to measure our opportunities to improve and our progress toward meeting objectives.*

Communication is the vehicle for demonstrating compliance. Regulations and legislation require specified reporting, but often the means for proving the validity of the required reports are not specified. That is where a progressive organization – building or maintaining its culture of compliance – will take the initiative to produce and keep the evidence of compliance. Electronic storage and retrieval is cheap when compared to the cost of making time for the regulators and auditors to visit and search out evidence of compliance. And the price of data management is miniscule compared to the potential damage an organization or its leaders may face when they cannot provide solid evidence of compliance.

In short, communication involves:

- a clearly understood commitment to do the right thing
- appropriate mechanisms in place to gather and maintain evidence of compliance
- actions rewarding compliance with the rules and punishing transgressions

Culture of Compliance™



- sufficient and flexible reporting capabilities to meet the existing and changing compliance reporting requirements

Confirmation is the way an organization ensures its progress is based on solid evidence.

Confirmation

Automated business systems will do what we tell them to do – right or wrong. A commitment to compliance includes building checks and balances into systems so they will reveal the evidence if they have been told to do something wrong. Authorization and authentication controls specify who is allowed to do what, and provide evidence of what they did. The history of corporate scandals includes numerous examples of individuals abusing their authority and systems that did not maintain evidence or support the reporting of such abuse.

Complex systems require monitors that can see through the complexity to identify the signs of processes or individuals operating outside the established boundaries. Confirmation includes not only recording events and reporting the required summary information, it also must include recording and reporting whenever established thresholds for normal transactions, risks, and controls are exceeded. Confirmation includes the transaction trails enabling management and auditors to trace activities and events through all steps of processing to their final effect on financial and management reporting with the capability to trace any reports back to the detailed transactions and events that affected them. Confirmation includes the ability to examine the elements of any management report to ensure their validity.

Confirmation includes the process for escalating notification for any significant event or exception to the level of management responsible for ensuring its appropriate resolution. And, it includes reporting on the results of resolution including confirmation of remediation. Confirmation also includes the proper balance of preventive, detective, and corrective controls, all with summary reporting supported by recorded detailed evidence.

Correction

Correction involves effective handling of incidents, but must also include identifying and addressing the root cause of each problem – not merely the symptoms. Imagine how foolish it would be to respond to hackers and viruses only after they have been detected in your systems.

Correction also involves noting those changes in business objectives, the market, the business environment, technology, and the regulatory and compliance environments that signal a need for corrective action at the strategic, tactical and operational levels.

As you consider the elements of communication, confirmation, and correction, notice that they do not vary across the diverse areas of compliance management. The same three Cs that apply to quality, health and safety, environmental, and privacy management also apply to Sarbanes-Oxley compliance. Organizations concerned about the costs and complexities of managing multiple compliance management systems and processes should adopt a combined compliance management solution within a single authority. A coordinated compliance management effort improves assurance and delivers economies from a compliance management system with a common database and reporting structure.

Benefiting from Compliance Management

Leading organizations know that measurement and reporting are essential to confirm that objectives are and will consistently be met. Effective leaders keep their team focused on the organization's goals and objectives. They benefit from understanding the strategic advantages in fostering a culture of compliance. Compliance leadership originates at the highest levels of the organization – the board of directors and senior executives. The Culture of Compliance must be pervasive throughout planning, execution, measurement and the feedback of results into planning.[2]

[2] See "Toward a Culture of Compliance – Building a Compliance Management Framework"; also on http://www.ibs-us.com.

In a culture of compliance, management and employees understand that a consistent approach to changing requirements and obligations is to measure and assess progress against objectives and requirements. Measurement is a standard component of effective management, and deviations from expected measurements are understood as matters for management attention. Within such an organization, assessments and audits are routine and regarded as a vehicle to gain additional insight into activities and opportunities.

Organizations that have embraced self assessment and regular audits experienced a relatively painless process of enhancing their monitoring and reporting activities to include Sarbanes-Oxley Act (SOx) compliance. To them, the COSO Internal Controls Integrated Framework was already familiar territory (it has been around for more than a decade) and it presented little challenge to adopt it into measurement and reporting processes. Leading edge organizations are also developing organizational analysis and learning tools to assess data patterns where known compliance breaches have occurred or are likely to occur (perhaps because they happened to another firm) and to identify data anomalies and other indicators to alert management and internal auditors to circumstances indicating established levels of tolerance are breached.

A Culture of Confidence™

Compliance Management has evolved rather quickly as a business "best practice." Until recently, compliance management may have resided within Quality, Environmental, or Legal departments. However, firms that embraced quality management concepts across the entire organization were the first to see benefits from regular assessments and audits. As compliance became the established focus of process management, compliance management systems similarly evolved to take in the expanding array of processes and activities subject to compliance.

Organizations are dynamic; they change over time in size, products, and services; and may grow from local to multi-national entities. The organization's systems must also be dynamic to cope with changes and to anticipate and respond to internal and outside forces. For years, progressive organizations have benefited from centralizing the management, systems, and data for diverse business processes that use and manage common information elements – customer data, inventory records, vendor files, etc. Customers gain confidence in an organization that recognizes them and can trace their transactions and history seamlessly across the array of varied products and services they may use.

An organization that makes it a routine practice to manage, measure, and report compliance will enjoy the confidence of employees, customers, business partners, and other stakeholders as they recognize the characteristics of integrity, consistency, and competence in all their dealings with the organization. In a culture of compliance and confidence, information systems management will also pursue a path of proven and reliable performance. It will also take maximum advantage of the opportunities afforded by available and emerging technologies.

What Are the Signs of a Culture of Compliance?

If you have to go looking for the signs of a culture of compliance, they probably are not there. But how do you know it when you see it? Remember the three Cs!

- **Communication:** Evident in consistent messages to personnel. Individuals know what is expected of them and provide vertical as well as horizontal communications.
- **Confirmation:** Expect processes and activities to be measured and results reported. Each position has a defined set of competencies, and performance is measured and rewarded. Monitoring and feedback are characteristics of all automated systems and procedures.
- **Correction:** Because of clear and consistent communication and confirmation, it is immediately known when a process, activity, result, or condition is outside of its acceptable parameters. Even trends and anomalous patterns are detected and information about them is directed into the measurement, reporting and response cycle. Things don't stay broken in a culture of compliance because the responsible parties are identified and held accountable.

A culture of compliance is evidenced by people working toward common and understood goals, with clear and consistent communication, efficient monitoring and reporting, and decisive action to investigate anomalies and take corrective action as needed.

Warning: Avoid Just the Appearance of Compliance!

When leadership senses a lack of commitment to

compliance, perhaps by seeing that others are rewarded for cutting corners, going for short-term profit, or reporting unsubstantiated results, they should suspect that their organization is satisfied with the mere appearance of compliance. The appearance of compliance exists when an organization reports according to requirements and makes statements that things are as they are supposed to be, but the confirmation and correction elements are so weak that they cannot provide evidence to the contrary. Tell-tale signs of corruption include the following:

- **Things are too good to be true.** If you never have a bad quarter (because that would not be living up to expectations), you soon violate a law of large numbers. The probability that measurements of a moving mean will be on the same side (+ or -) of the moving mean line for seven consecutive measurements is two percent (2%).[3]
- **Problems do not rise to the surface** – even to report that they have been resolved. If the message from above is "Only good news, please," then subordinates will seek to mask any problems – including non-compliance. Be very suspicious if you never get bad news.
- **You cannot drill down to the details that support compliance reports.** Compliance management cannot be viewed as a set of simple evaluations, each having a binary "compliant" / "non-compliant" result. It must be possible for stakeholders to straight-forwardly answer "who", "why", and "how" questions about compliance results. Compliance failures or problems are driven by constituent compliance components. A compliance management system that obscures result drivers does not serve its purpose. An effective compliance system will not only "float" the significant results of lower-level key performance indicators, it will also let stakeholders trace the factors that underpin overall compliance.

Real compliance includes controls and measurements with solid reliability whether they demonstrate desired results or results that are borderline or even below target levels. This may occur for many reasons including problems that have not yet been fully resolved, risks that materialized in a manner other than expected, mergers and acquisitions, and the inevitable results of human error and omission. An effective compliance management system allows management to identify problem areas and assess the appropriate priorities for resolving them and/or relying on compensating controls.

> If you've been listening, you know it's not enough to have policies. It's not enough to have procedures. It's not enough to have good intentions. All of these can help. But to be successful, compliance must be an embedded part of your firm's culture.
>
> From a speech by Lori A. Richards, Director, Office of Compliance Inspections and Examinations, U.S. Securities and Exchange Commission, April 23, 2003.

Conclusion

As you build and maintain your Culture of Compliance, be sure to reward problem solvers at least as much as those who report only smooth sailing. Be sure that employees realize that management will not accept the covering-up of problems, especially non-compliance. And be sure that the systems in place allow management, auditors, and regulatory examiners to look into the facts, details, and numbers that make up compliance reporting. It is better to know about problems from the outset than to be surprised to learn your compliance system or culture is flawed after reading your company's or maybe your own name in a negative headline or on a subpoena.

As the management team operates the organization's daily business, it needs the confidence it can only receive from a Culture of Compliance. The organization also needs the benefits that accrue from a well conceived and executed compliance management program featuring continuous improvement. The best solution involves coordinating the diverse compliance management activities through a single management entity equipped with a solid mandate and a compliance management system that is capable of combining similar activities for efficiency and the maintenance of a comprehensive database of compliance requirements. Only in such an environment can the governance bodies be assured of effective and sustainable compliance.

[3] The statistical rule of sevens.

Executive Compliance Management Checklist

- Executive management and the board of directors play an active role in establishing and monitoring compliance strategy and the culture of compliance.
- Compliance is a high priority for the organization.
- The organization has designated a Chief Compliance Officer.
- The organization provides and maintains clear and comprehensive compliance guidance for each functional unit and for the ways the functional units interface with each other and with the organization's leadership.
- All business units and processes are included in the compliance strategy.
- The compliance management function is adequately staffed and appropriately structured.
- Compliance management is efficiently supported by centrally managed technology tools including databases, processing, monitoring, analytics and reporting.
- The compliance management system interfaces smoothly with other systems for coordinated information sharing and control.
- Compliance controls are well documented for internal and external purposes.
- All staff members are aware of the compliance requirements and qualifications for their positions and are kept qualified by educational programs and demonstrated proof of competence.
- Staff members know the avenues to advancement and the qualifications necessary to attain promotions and other rewards, including the compliance responsibilities of each position.
- Adherence to compliance requirements is integral to the organization's reward structure.
- Violations of the compliance policy result in punitive measures.
- All out-of-compliance conditions and compliance violations are immediately reported and monitored until effective corrective actions are applied.
- Compliance is independently assessed by internal and/or external auditors on a recurring basis.
- Audit assessments are planned and coordinated to ensure consistent coverage of areas of greatest risk and less frequent attention to areas of lesser risk.