How to Build and Maintian a "Culture of Compliance"™

Charles H. Le Grand, CHL Global Associates

Sponsored by IBS America, Inc.*

http://www.ibs-us.com

How to Build and Maintain a Culture of Compliance i
Overview 2
Enterprise Risk Management 2
Effective Process Management 2
Product of Corporate Governance 2
Goal Oriented 2
Approriately Controlled 2
Accountability Defined and Enforced 3
Qualification 3
Appropriate Technology 3
Document Control 4
Preventative, Detective and Corrective Actions 4
Compliance Assessments 4
Sustainable Compliance and the Compliance Management System 5
Implementing a Compliance Management System 5
Communication 5
Confirmation 5
Correction 5
Matching the Compliance Management System to the Organization 6
Conclusion 6
Appendix A - Example Requirements for a Compliance Management System 7
Document Control 7
Elements of Document Control for Compliance Management Systemsm 7
Preventative, Detective, and Corrective Actions 8
Compliance Assessments 8
Reporting 9

*IBS America, Inc. has been a leading provider of compliance management solutions since 1994. Copyright 2005 by IBS America, Inc. All rights reserved.

Overview

Compliance should be the ethical core and integral to the day-to-day operations of an organization. To regard compliance as a project or a target is to foster a lack of acceptance and provide a clear message that we are only doing these things because we are forced to do so. Compliance must be specified in corporate policy and the ethics program, clearly and consistently communicated to the organization's people, owned and operated by qualified staff, inherent in measurement and management processes, evident in rewards and punishment, and supported by appropriate technology.

This report provides a concise and clear framework for building and enabling the compliance management culture and processes. For more information on what a culture of compliance is and its main components, see Building a "Culture of Compliance"™ for a "Culture of Confidence"™ (also by Charles Le Grand).

Enterprise Risk Management

Compliance activities must begin with identifying specific risks that can arise in each strategic area and then follow with the controls and communication to effectively address them. Risks apply generally to the organization and its objectives, specifically to individual processes and activities and are subject to constant change. Risk management is integral to compliance management. Specific compliance risks may also be elements of required reporting, as in the case of the Sarbanes-Oxley Act, and regulatory examiners may require an explanation if they notice that some risks are not included in reports.

In some organizations there is confusion about the differences between risk management and compliance management. Risk management is integral to an organization's success. Each organization has its own risk appetite requiring that risks be bounded, managed, and reported in certain ways. Those organizations that manage other people's assets, including sensitive information, are also required to manage in accordance with those people's risk tolerance and to report when risk boundaries have been breached. Failure to comply with risk management requirements is a compliance risk. And compliance sets limitations on risk management. Risk management and compliance are closely interconnected, but they are not the same process.

Effective Process Management

Process management is much more than something good managers do instinctively. Just as gifted musicians must sharpen their skills through a rigor of training and practice, the best managers will continuously enhance their skills and knowledge – including understanding and applying available tools and technologies to increase their effectiveness.

Product of Corporate Governance

Commitment to a culture of compliance must be communicated from the board of directors and senior executives throughout the organization. Then these leaders must be attuned to the reporting of results and aware of the subtle shifts in information that can signal opportunities, warnings, or other calls to action. The leaders will also let the entire organization know that rewards are based on results that are measured and reported, within the acceptable level of risk, and according to the organization's code of ethics.

Goal Oriented

Process management practices that maintain their goal orientation will contribute to confidence on the part of stakeholders. Confidence in the organization will contribute to improved visibility for such practices as prudent risk management, responsible citizenship, and appropriate response. The consistent application of process management will be observable in the organization's language and terminology, the things it measures and monitors, and even the attitudes of employees. Employees as well as the leaders will understand that compliance represents consistent practice – not just a project or a technology solution. And actions do speak louder than words. Many dramatic "compliance" problems in recent years have resulted from deeds by top management who were fully aware that they were not ethical.

Appropriately Controlled

Processes do not take place in perfect environments. Just as risks must be identified for all areas and activities, so an integrated framework of controls must be in place to prevent, detect, and correct against risks as they

materialize. In addition, the controls must frequently adapt to the changing environment and to the introduction of new risks. Controls are all the things you would not have to do in a perfect environment including keeping track of all the things that can go wrong and measuring and reporting all deviances from the desired state.

Accountability Defined and Enforced

A culture of compliance depends on specific individuals to be accountable for managing each element of compliance and the compliance systems and processes. Accountability takes into consideration the need for shared responsibilities as well as compensating controls. A weakness in one area should be detected by the controls and accountability in another area. While morality may be defined by what people will do when no one is watching, compliance management depends on people knowing their activities will be monitored and traced back to them.

A traditional accountability technique is to force collusion if someone wants to practice fraud or deception. The theory is that improper actions will be less likely to get started if two or more persons must agree to initiate them, and they will be harder to keep secret.

Qualification

Competence is an essential element of a culture of compliance. You would not trust an incompetent driver with your car, so why put incompetent staff in a position where they can negatively impact an organization's culture of compliance. Organizations must ensure their people are competent to reliably perform their tasks and meet their responsibilities. Further, as change is constant, each position will have a set of competence requirements specified for individuals qualified or qualifiable to perform the duties of that position. And each employee will have an associated record of their qualifications, experiences, and credentials.

Training is essential to maintaining competence, so positions and employees will also have objectives to meet ongoing training and development requirements. When appropriate, training programs will include participant assessments of the program's effectiveness, and testing to indicate the extent to which the training was assimilated by each individual.

A compliance management system should maintain records of position requirements and employee qualifications, be capable of matching qualified employees with available positions, and identify qualification opportunities and objectives for employees. Further, it should keep up with qualification requirements of outsourced service providers, suppliers, partners and customers if applicable.

Appropriate Technology

An organization's technology management plan must not only provide for data, processing, analytical capabilities, and communications – it must also address opportunities available in new and emerging hardware, software, and communications capabilities. And it must look ahead to emerging and developing technologies that will continue to improve the organization's capabilities and advantages.

Some organizations will have a strategy of adopting new technologies only after they have been tested and proven by leading-edge companies. In such cases, the technology strategy must also include observing organizations that have implemented new systems and features, looking for success stories. In all cases, it will be important to know about available systems that can enhance the capabilities and benefits from effective compliance management. Just as organizations are expected to stay abreast of the latest security capabilities, malware protection, and patch management, so a culture of compliance must include implementing available, cost-effective systems that can measurably improve compliance communication, confirmation, and correction capabilities.

Compliance management systems have grown to address not only the individual elements of compliance, but also the tracking of requirements across multiple types of compliance and across all areas and levels of the organization. Compliance management systems control the recording of information and documentation, ensuring it is available as needed, and in the appropriate form and context. Embedded monitoring and analysis of processes and specific transaction types enable the identification of anomalies and trends that can indicate problems or opportunities.

Document Control

Without evidence, there is no compliance. Document control is the central repository of compliance and control requirements and it is the source of compliance evidence. While the actual measurements and reporting may result from application systems processing the transactions and activities for an area of business (accounts payable, inventory management, manufacturing process control, human resources management, etc.), the ongoing maintenance of compliance information and documentation is a key role of the compliance management system.

Documentation Maxims

If you did not record and measure it, it never happened.
If it cannot be measured, it cannot be managed.
If you do not have records of

- measurement
- inspection
- detection of problems
- and correction

you have no basis for demonstrating performance or for proving success or failure, innocence or guilt, custody or ownership, authorization or authentication.

Document Control includes a directory of all types of documentation maintained by the Compliance Management system. As in any data directory system, it will identify data type, category, owner, approval authority and more.

In the case of documents on paper or similar media, document control includes images – duly referenced, and available electronically on demand or automatically in support of compliance reporting.

Document control is a major element of automated systems supporting compliance management. In addition to managing the availability and versions of compliance-related documents such as evidence and reports, the document management system should also contain the compliance control requirements and reference them to the compliance management documents.

Preventative, Detective and Corrective Actions

Controls are those actions you would not have to take in a perfect environment. If no one ever made data entry errors you would not need edits. If no one ever fudged numbers, you would not need analytics to spot the anomalies that exist when people make up their own numbers. (Yes, there are statistics and laws of large numbers that are typically violated when people or companies inflate earnings, hide debt, or otherwise cook the books. You just have to know how to look for them – and have a will to do so.) And if things did not break or outlive their productive life, you would not have to fix or replace them.

A culture of compliance is attuned to the things that can go wrong. It notices deviations in patterns and takes steps to identify and respond to the causes (not just address the symptoms). And it identifies opportunities as well as problems in data patterns.

You may not know it, but an employee newsletter is a preventive control. Well informed employees are more comfortable, competent, and content in their positions. They know the mobility opportunities and the actions they must take to qualify for them. Similarly, whistle-blower systems, compliance hot-lines, and suggestion boxes are elements of appropriate communications. Signs warning of restricted areas, pictured identification cards, motivational and educational posters, news of accomplishments and awards, and yes, even ready availability of policies and procedures – all are signs of an organization that takes communication seriously.

Compliance Assessments

"Where were the auditors?" How many times have you heard that? In a perfect environment, you would not need auditors. Auditors typically follow predictable patterns of analyzing business processes, identifying controls, assessing controls for appropriateness and reliability, testing those controls deemed likely to be sufficient, and testing the data for potential errors in areas where the controls are determined to be incomplete or ineffective. Compliance assessments are based on the assumption of effective controls. If controls are found to be inadequate, they will not comply with requirements, and the auditor must so report. However, historically management had the option of ignoring the auditor's

recommendations to resolve control deficiencies.

Now that the Sarbanes-Oxley Act requires management reporting on internal controls, auditors have the responsibility to attest to management's assertions regarding the reliability of controls. And auditors must independently test those controls deemed significant to financial processing and the reliability of financial reporting.

In order to ensure the most critical controls are identified and evaluated, management and auditors will rely on an assessment of key risks the organization faces. Thus, risk assessment is a critical element of control assessment, and control assessment is a critical element of SOx compliance. Ideally, management will perform effective risk analysis and risk management and the auditors can agree with management's conclusions. But when auditors identify weaknesses in controls and/or errors in data, it becomes incumbent upon management to respond with strengthening of both controls and assessment to prevent, detect, and correct any future problems of that type (through routine confirmation and correction). No longer can auditors expect to find last year's problems still unresolved.

Sustainable Compliance and the Compliance Management System

For many years organizations have invested in compliance processes and systems and most have viewed compliance as a separate matter for each area of compliance (internal policies and procedures, quality, health & safety, privacy, employment …). SOx, however, specifies "internal controls" as a compliance subject for all internal controls relevant to financial processing or the reliability of financial reporting. Thus risk management becomes a specified area of internal control because it seeks to identify and protect against risks that could have a significant impact on finances and financial reporting.

Many companies regarded SOx compliance as a project to identify and document internal controls and assess their effectiveness. But business models and environments are not driven by regulations. They have their own dynamic with frequent impacts on business processes and controls. SOx requires reporting of changes to controls and reassessment of effectiveness. So viewing SOx compliance as a period-of-time project creates the challenge of revisiting controls documentation and monitoring for each change, and the risk of non-compliance continues to increase instead of decreasing due to efforts applied, lessons learned, and documentation prepared.

Implementing a Compliance Management System

The compliance management system should be centrally controlled and administered to ensure participation and cooperation from everyone involved in the process. Moreover, system design should be in alignment with the communication, confirmation and correction objectives.

Communication

Reporting is key for satisfying compliance requirements and therefore must be a primary deliverable from the compliance management system. And in routine operation, the system will provide management insights to each area of compliance through summary level information as well as the ability to drill down to the most specific details of compliance management.

Confirmation

The compliance management system records the results of risk assessment, risk monitoring, control monitoring, statistical and other analyses of compliance data maintained. Ideally, the compliance management system will combine the data management, analysis, and reporting for all areas of compliance.

Correction

Corrective actions are not always immediate. They may be subject to mandated schedules or management discretion. They may involve lost opportunities for failure to comply with internal objectives and they may involve sanctions or penalties for failure to comply with external requirements. Whatever the need, the Compliance Management system must provide recording and reporting and include reminders of approaching deadlines.

The lists in Appendix A provide examples of information to be maintained and summarized by a compliance management system. Specifics of information elements, regulatory and other requirements, monitoring, analytics, exception handling, reporting, and other details of compliance management will be germane to the individual areas of compliance. The system should

provide the flexibility to analyze and report data according to the individual and changing needs of compliance management personnel, executives, and governance bodies.

Matching the Compliance Management System to the Organization

In any given organization, you can expect to find areas of compliance management in varying degrees of automation and completion. You may find some compliance systems that have long-since matured into process management rather than project management.

Matching the organization's systems plan to compliance management may involve seeing the organization's compliance efforts as a series of concentric circles beginning with the most mature database of compliance information and expanding to take in areas of greatest risk and/or opportunity as resources and requirements allow. Most organizations will not start from scratch but will develop a plan to interface existing compliance systems. Then they may establish long-range objectives to combine all compliance management efforts into a single system.

As in other process management systems, it is desirable for compliance management to provide a single-source solution. A coordinated compliance database can maintain all compliance requirements regardless of their source. The requirements database can identify the source of requirements but, more importantly, map them to all applicable areas. A major benefit of a single compliance database is the ability to monitor a high-level heat map and drill down into the various environments and elements of compliance.

Conclusion

Compliance management puts the culture of compliance into practice for the benefit of the organization and its stakeholders. Efficient compliance management also looks at the common elements of compliance and coordinates them within a common management structure supported by a centralized compliance management system that is capable of interfacing with all of the individual areas of compliance.

There is no substitute for the value of an ethical culture of compliance, and ethical leadership will understand the need for compliance and put it into practice whether or not it is mandated by external authorities.

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 sush as education
- Reinforced in incentive systems
- Given force thorugh the treatment of transgressors
- Integral to information systems and their use and management
- Inseperable from the organization's structure, processes, and management style

Compliance Management encompasses enterprise risk management, addressing the risks that arise in each strategic area. It:

- Establishes control points for the risk elements
- Ensures controls are well documneted 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.

Appendix A - Example Requirements for a Compliance Management System

Process Management

Automated systems provide the basis for accomplishing business processes and communicating results. They serve all levels of the organization with horizontal as well as vertical communications. A system to provide coordinated management of compliance processes across all areas of the organization is an optimum compliance management solution. But in a culture of compliance, consistent communications will also be evident across all systems used to support the organization. Process support elements for a compliance management system include:

- **support corporate governance**
  - clear communication from governance directives
  - clear, consistent, and flexible reporting of results
  - executive summary with drill-down capability
- **goal oriented**
  - build and maintain confidence
    - customer, investor, employee, public
  - improve visibility
    - prudent risk management, responsible citizen, appropriate response
- **consistently applied across enterprise**
  - observable in environment, terminology, measurement, and reporting
- **not a project or a technology solution, but ongoing process management**

Document Control

Automated systems are capable of storing, categorizing, monitoring, summarizing, and reporting on vast quantities of complex and interrelated information. When you consider the types, complexities, similarities, and differences in the data needed to manage compliance, it should become obvious that the only way to successfully manage the data is with a system specifically built for that purpose.

Elements of Document Control for Compliance Management Systems:

- document directory
  - type, category, owner, approval authority
- document images
- compliance and control requirements
  - laws, regulations, standards, agreements, policies
  - quality, environmental, reporting, privacy, security
  - specific objectives and responsibilities for control
  - control processes

- design and change specifications
  - compliance management strategies
  - functional requirements (including internal control questionnaires (IQC) responses)
  - release schedules
  - approval authorities
- review and audit
  - requirements
  - checklists, internal control questionnaires (IQC), regulations, schedules
- related documents
  - email, instant messages, web notices
- surveys and responses

Preventative, Detective, and Corrective Actions

- qualification
  - personnel requirements
    - employment and employee screening
    - ongoing competence (link to training and communication)
    - routine requirements (password maintenance, clean desk)
    - discipline and termination requirements
- physical and logical requirements
  - area security
  - off-hours surveillance
  - intruder alerts and responses
  - information security
  - access controls
  - segregation of duties
  - system and network configuration
- requirements for customers, suppliers, business partners
- requirements from customers, suppliers, business partners
- protection of customers, suppliers, business partners

Compliance Assessments

- risk assessments
- internal quality assessments
- management assessments
- routine monitoring
- internal auditing

Reporting

- required compliance reports
- internal management reporting
- executive dashboards
  - window to each and combined compliance summaries
  - drill-down to specific documentation
  - observation of continuous monitoring objects
  - action items
    - to do lists - tasks and tracking
    - corrective and preventative actions (CAPA)
    - links to other systems and reports
  - status reports
  - schedules and deadlines
- collaboration
  - information sharing across compliance areas
  - FAQ (frequently asked questions)
  - cross-reference of similar and related requirements and activities
- architecture for sustainable compliance