



Commentary

April 2008

A Culture of Compliance: Strategically Managing Compliance Efforts

By James Barrow
Global Information Protection Business Continuity

In today's business environment, organizations are increasingly required to abide by one or more regulatory compliance programs. For most organizations compliance with each regulatory requirement is viewed as a separate and distinct activity. Many organizations treat compliance programs in an erratic fashion, meaning that there is no consistent process; the organization only concentrates on compliance efforts as deadlines loom, and approach them with a "firefighting mentality." Using this reactionary mode many organizations are doing all they can just to stay ahead of the next regulatory requirement. Most organizations have not capitalized on the paradigm shift to enable their compliance efforts to permeate their normal business processes.

In this erratic "firefighting mentality," compliance often competes with other projects such as political or financial driven ones. As organizations realize the negative consequences that may be imposed for lack of compliance (for example, monetary fines), compliance is suddenly propelled to a priority project. This often leads to poor decisions involving time and money being made in order to meet the deadline.

Incorporating the paradigm shift towards a culture of compliance allows the business to view compliance in a new light. This new perspective is to view validation with compliance programs as the ability to integrate the requirements of compliance into the day-to-day business operations of the corporation. Taking this built in approach means that the organization has incorporated compliance into the business culture.

Once this culture has had time become fully integrated and mature within the company, compliance is no longer seen as a stress laden pass or fail event. Building this culture allows the business to plan ahead for compliance related activities. This prior planning allows for a more normalized allocation of time and money throughout the year. Once the organization has decided on a paradigm shift from unpredictable to cultural compliance, decisions are made in a more attentive manner. Selection of the appropriate controls, equipment and solutions for compliance are usually more rational with long-term business objectives in mind.

Developing a Culture of Compliance is a Top-Down Strategy

For an effective culture of compliance to be established and thrive within an organization requires C-level commitment and resources. Compliance activities cannot be reserved for small groups within the organizations such as senior management, audit or security. Nor can a culture of compliance thrive within companies where individual groups or divisions have established strong silos. Compliance activities must be pervasive throughout the organization, and cross all functional areas, (for example, Technology, Human Resources, Legal). The directives established at the top level of the organization must be fully communicated throughout the organization. Failure to do this will limit the overall success and effectiveness of developing this new organizational culture.

Leveraging Existing Controls

PCI, like other regulatory requirements, was developed to meet a specific need. It had been identified that merchants were failing to place the proper controls around sensitive cardholder data within their environments. Leveraging existing controls introduced from other regulatory programs such as HIPAA, or SOX can help to reduce costs associated with programs such as PCI.

Building a culture of compliance will allow the organization to easily mitigate risks and meet regulatory requirements. Having this culture of compliance in place provides the organization to leverage three key components; people, processes, and technology to provide an operational framework that is effective, measurable, and repeatable and delivers long-term results. Having this culture of compliance established within the organization brings organizations closer to reaching business-critical corporate objectives, and removes the cyclical firefighting mentality.

Benefits

Organizations that develop a culture of compliance should readily realize the benefits of having such a strategic plan in place. Some of the benefits that should be easy to recognize are reductions in inefficiencies, as well as the ability to leverage controls that may have been implemented from other regulatory programs.

Controls introduced in order to achieve regulatory compliance often identify and help to rectify inefficient business and technology processes. Additionally, these controls help to establish monitoring programs to ensure that once inefficient processes are identified and corrected that they remain in a state that allows for continuous improvement.

As the culture of compliance is established and matured within the organization, monetary benefits should also begin to be realized. As compliance efforts become unified and compartmentalization of compliance efforts are removed, the company should see reductions in hours spent on compliance as well as reductions in overlapping solutions that are purchased.

Conclusion

As organizations move from a mentality of erratic compliance validation to a culture of compliance, several benefits can be realized. These benefits include items such as better compliance planning, cost reductions from a decrease of introduced redundant solutions, and overall hours dedicated to compliance. Finally, a culture of compliance will allow the organization to spend a larger amount of time and resources on business-critical functions.