



Sustainable Compliance

Pat Slagle, President, In-Depth Security

Introduction

Meeting and maintaining compliance with regulatory and business entities is both complex and expensive. Consider this - a new survey released in June of 2005 shows that a majority of firms surveyed (74%) must comply with more than 5 laws and regulations. And according to the SEC, more than \$4 billion has been spent to date on SOX compliance alone. So whether it's SOX, GLBA, PCI or HIPAA compliance you've achieved, don't waste the significant expense and effort expended. You can minimize the cost and effort of sustaining compliance by establishing an effective program that supports multiple requirements.

In order to build sustainable compliance, you should focus on the following:

1. Maintain the momentum Executive management needs to deliver overt and **visible** support. If they don't buy into the program, neither will anyone else. How?
 - Key points
 - Evangelize ethics, internal control and personal integrity
 - Communicate and visibly support policies assigning authority and responsibility
 - Don't tolerate ethical violations
 - Publicly reward successes
 - Enforce accountability
2. Implement and monitor self assessment processes to reinforce responsibility and accountability.
 - Key points
 - Provide clear expectations
 - Link to specific business processes and controls
 - Audit periodically
3. Establish an ongoing risk identification process.
 - Key points:
 - Apply risk based testing and focus on deficiencies identified from previous test results
 - Focus on controls that significantly impact quarterly results.
 - Identify, support and enable risk specialists
 - ...within business units
 - ...or as a separate entity
4. Formalize a reporting and escalation process.

- Key points
 - Deliver bad news fast to the right people
 - Escalate fast

- 5. Manage and assess IT related risks and controls.
 - Key points:
 - Identify and streamline overlapping or redundant controls
 - Continue to assess IT related risks and identify controls to mitigate those risks
 - Identify and implement appropriate technology solutions for
 - Document sharing
 - Controls evaluation
 - Controls automation

Summary

Sustainable compliance can be achieved by focusing on these activities but not without some challenges. Independent, objective and appropriately skilled resources are key to the successful execution and maintenance of these efforts. For information on how to supplement your efforts with security experts, services and products, please visit In-Depth Security at www.indepthsec.com.