Compliance Reviews and Mitigation

Regulatory requirements related to security have changed dramatically over the last 7 years and the changes are likely to continue. Whether it's the Health Information Portability and Accountability Act (HIPAA), the Gramm Leech Bliley Act (GLBA), the Sarbanes-Oxley Act (SOX), California Senate Bill 1386 (SB1386), or the myriad of other international, federal, state, and local regulations, regulatory drivers are increasingly and more directly requiring stronger management controls over security functions within companies.

SOX 404 as an example:

The best recent example of the regulatory drive for controls is the rush to compliance with SOX section 404. SOX 404 is the first law in this space to really have teeth. The punishment for executives of public companies who fail to meet the requirements of SOX 404 is federal prison.

The language of the law really has no specific requirement for security controls of any sort. However, the requirement for financial controls combined with the use of information technology in accounting and the regulators' interpretation of the law leads to more specific requirements. The most specific requirement identified in the interpretation is the adoption of the recommendations of the Committee Of Sponsoring Organizations (COSO) of the Treadway Commission. These recommendations identify control requirements that are not specific in any way. But they do require that top management:

- Set control objectives
- Identify events that can cause serious negative consequences
- Assess risks associated with those events
- Respond to risks using a risk management strategy
- Deploy control activities appropriate to those responses
- Communicate control requirements effectively throughout the enterprise
- Monitor compliance with those controls

This must be done at the entity, division, business unit, and subsidiary levels as part of strategy, operations, reporting, and compliance.

As enterprises rush to comply, they are required to have their accountants attest to the adequacy of their internal controls. Their accountants are also rushing to help them comply, but the lack of skilled experts and specific guidance in analysis of control standards like COSO means that there isn't enough expertise to do the job properly. So accounting firms choose more specific control standards, like CoBit, create checklists, and have inexperienced auditors use them to review enterprises. Enterprises or their employees may misrepresent the situation and are often less than forthcoming, making the process adversarial in nature, and making it impossible to accurately validate the results. The combination often produces results that are expensive to implement, ineffective at managing risk, and don't really meet regulatory or enterprise requirements.

Service Summary

We are usually brought into the compliance picture before an audit as a pre-audit reviewer, after preliminary audit results as a mediator to reconcile disagreements before the audit is finalized, and after audit completion to help mitigate shortfalls.

- **Pre-audit:** In the pre-audit role, the most effective process is an information protection posture assessment (IPPA) with SOX emphasis. This assessment rapidly identifies the issues that have potentially serious negative consequences and are inadequately controlled, identifies general control limitations that should be mitigated, and does a comparison with COSO and more detailed control standards to give a sense of the situation and paths to mitigation. IPPAs take from 30 to 90 days to complete and are usually scheduled 30-45 days in advance.

Illustration 1 - The COSO Cube

- **Mediation:** In the mediation role, we are usually contacted over specific issues where the accountant and the internal experts disagree. These are usually the result of inconsistencies in the requirements, inadequate understanding of risk issues, checklists that are misapplied, decision-makers who don't believe results, and so forth. In these cases we are typically engaged on a retainer basis to negotiate a reasonable solution that the auditors can attest to and the enterprise can implement.
- **Mitigation:** In the mitigation role the challenge is often more daunting. We are called on to meet very tight schedules for such things as complete policy rewrites, creation of a full spectrum of activities for a Chief information Security Officer (CISO), or addressing internal power struggles. These services are usually provided through pre-defined service offerings such as our policy reconciliation and rewrite service or our CISO service. They involve standard processes at standard pricing with add-ons based on time and materials.

Whether it's SOX 404, HIPAA, GLBA, SB1386, the European Union safe harbor, or any other requirement for regulatory compliance involving security-related issues, we have the people and the experience to efficiently and effectively resolve the issue in a timely and professional manner.

For information on assistance with regulatory compliance issues, contact your sales representative for a scoping call and we will generate a statement of work.