Policy Assessments

Apples and Oranges

Most legitimate information security consulting firms offer various policy assessments, ranging widely in scope and price. Our clients often complain of the difficulty in comparing one proposal to the next. To solve this problem, **infotex** has always encouraged our clients to focus on the certifications brought into the policy assessment process. Once assured that the appropriate certifications are being used (currently CISSP or CISA for most Information Security assessments), clients can then compare costs with a relative understanding that the quality of work will be equal. The client can then focus on the actual process being proposed, which will still greatly differ from one consulting company to the next. The only exception to this would be a full-blown Information Technology Audit, in which the process used by all firms will be relatively equal (though different firms may still focus on different issues, based on perceived risk).

Compliance Programs

We like to encourage our clients to view Information Security Policy Development as a journey along a "Compliance Path" that spans two to three years. The compliance path must be designed based on the ultimate goal of managing risk. With a risk-based approach to compliance mitigation, our clients (and more importantly their Board of Directors) can be assured that policy development follows a cost-effective and business-oriented approach. Because of the fact that different organizations are in different positions along the "compliance path" related to policy, we have created series of Policy Assessments that can be used individually or as an orchestrated method of achieving compliance.

Assessment Series

The series starts with an overall Information Security Posture Assessment, and each additional assessment type drills deeper into the overall health of your operational and information security controls. With some minor variations for specific frameworks and/or regulations, the assessments we offer include:

- Information Security Posture Assessment
- Targeted Policy Gap Analysis
- Comprehensive Policy Gap Analysis
- Data Flow Risk Assessment
- Information Technology Policy Audit
- CobiT Policy Audit (or ISO17799)

Financial institution management should implement satisfactory control practices as part of its overall IT risk mitigation strategy. These practices should include adoption and enforcement of IT policies and standards.

- FFIEC Management Booklet

Information Security Posture Assessment

In this "Control Self-Assessment," intended for organizations at the beginning of their compliance path, our CISAs provide basic training to the management team. We then walk the team both individually and as a group through a set of questionnaires which are fed into a report that helps the organization design a compliance path. The process, based on FFIEC guidelines, establishes metrics that can be used by management over time to demonstrate risk mitigation via policy development. This approach minimizes management team involvement as well as consulting fees.

Policy Gap Analysis

In this approach, we interview your management team and several other persons in your organization. We solicit documentation of policies and procedures and then run submitted information against checklists that we have developed based on the FFIEC guidelines. We then deliver a report with detailed deficiencies noted in policies and procedures as well as suggested remediation. The report includes an executive summary as well as a detailed "policy gap matrix" that applies a risk analysis on each deficiency and establishes metrics that can be used over time to measure remediation (and inherent risk). We can target a policy gap analysis to specific policies or program, such as Acceptable Use Policies or Vendor Management and/or Incident Response Programs.

Data Flow Risk Assessments

This policy review focuses on the very wide-ranging issue of Data Ownership, Access Management, and Data Classification. Unlike a targeted policy gap analysis, this assessment involves al data owners and is a development engagement as well as an assessment.

Information Technology Policy Audit

A full blown Information Technology Policy audit includes an Information Security Posture Assessment as well as a Comprehensive Policy Gap Analysis. However, it also goes so far as to test the controls in existing audits. This approach can be taken with a specific framework (such as CobiT or ISO17799) as the over-arching audit control guideline, or can focus on the FFIEC or HIPAA guidelines, which is what most smaller, privately held financial institutions prefer.