March 12th, 2009 Chapter Meeting – HIPAA, SOX, PCI, GLBA

Presented by LogiSolve

HIPAA, SOX, PCI, GLBA.....In today's corporate environment, businesses are facing increasing regulation affecting the corporation's bottom-line. As a result corporate policies and standards, once just a necessary, but largely irrelevant cost of conducting business, are increasingly becoming a companies first line of defense in the face of the new regulatory environment.

As such, it is critical that policies and standards be aligned with regulations and industry standards. But who in the firm monitors regulations and determines when updates are required? Who ensures the policies and standards are being followed? How does one establish traceability between regulations and the requirements mandated?

This presentation will explore solutions regarding:

- How to assess current corporate policies against current regulations
- Establishing a framework promoting compliance
- Measuring , remediating, or accepting risk as appropriate
- Developing a comprehensive compliance program incorporating the regulations and / or industry standards

HIPAA, SOX, PCI, GLBA.....IN TODAY'S CORPORATE ENVIRONMENT

Establishing IT Risk Management by Garrett Dietrick

Establishing Risk

Today we are going to cover four key areas which encompass

Establishing a Policy Framework

What is the state of your corporate security

Establishing a Policy Framework

Policy

- Over the course of the past 5 years corporate

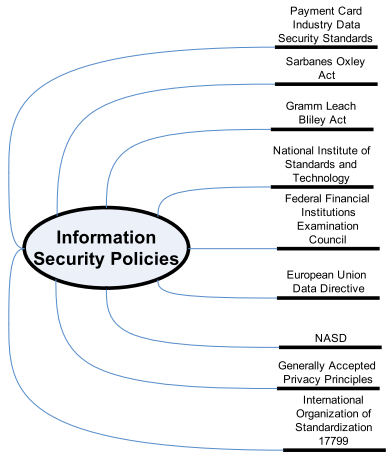
Establishing a Policy Framework

Identifying and understanding the regulations imposed on your organization.

I comply with regulations, so I must be secure right?

Wrong!

Then where else can I look for guidance?



Establishing a Policy Framework

Take the first step, performing a gap analysis:

- Select a

Establishing a Policy Framework

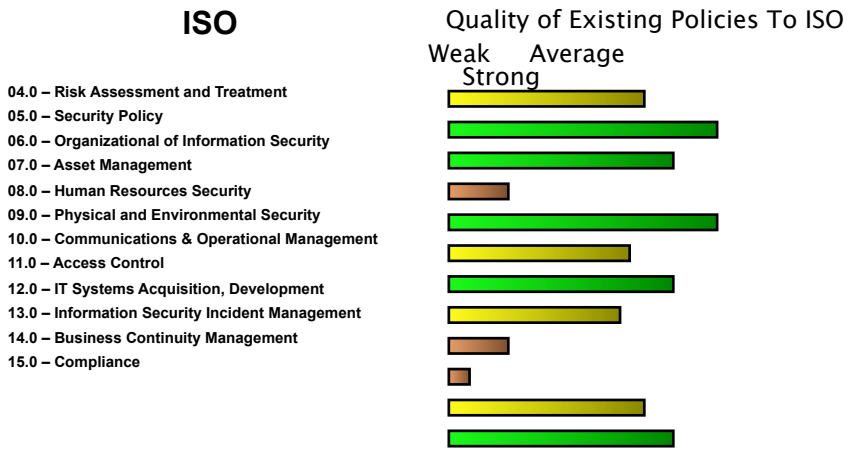
The Gap Analysis will help determine the extent to which

Gaps identified are then so scrutinized to determine

Improve the Content

- Organiz

Establishing a Policy Framework



Establishing a Policy Framework

- 11.0 Access Control
  - 11.01 Business requirement for Access Control
    - 11.01.01 Access Control Policy
  - 11.02 User Access Management
    - 11.02.01 User Registration
    - 11.02.02 Privileged Management
    - 11.02.03 User Password Mgmt
    - 11.02.04 Review of User Access Rights
    - 11.03.01 User Responsibilities
  - User Responsibilities
    - 11.03.01 Password Use
    - Etc. Etc. Etc.

Quality of Existing Policies To ISO

Weak Average Strong

Gap Analysis Summary

- 50 Unique Control Standards in ISO
- 27 Control Standards Map to Corporate Policy
  - 8 Modified / Improved Content
  - 12 New / Added
  - 11 Not Mapped and Not Used

Key Gaps Identified

- No Policy on User Responsibilities
- Password Management does not meet requirements

Establishing a Policy Framework

- The next major task is to identify owners of each policy section i.e. Information Security, Physical, Security, Human Resources, etc..
- These owners will serve as resources to identify current business processes and owners of the policy content.
- After the owners have finalized their content, it is best to have the new policy reviewed by other departments including:
  - Legal
  - Privacy
  - Compliance
  - Audit / Assurance
    - Note: Keep a file with all of the requested changes and responses.
- When content is final, obtain an official sign off from all owners and reviewers; this ensures:
  - Authority and Accountability

Establishing a Policy Framework

Establishing Risk

Now we are moving on to the second phase: Performing Risk

Performing Risk Assessments

- Why are Business Analysts interested in risk assessments?
- What are organizations currently doing?
- Is there one method which should be used over another?
- Where do we start?

Performing Risk Assessments

- Risk Assessments must keep one thing in mind, which is RISK.
- The first step is to identify the controls to be tested for a risk assessment. The framework used in policy creation is a logical starting point. Key questions to ask before embarking on a risk assessment include:
  - What are the organizations main concerns when it comes to risk?
  - What is the appetite or risk tolerance of the firm?
  - What is the firm's approach in dealing with findings from the assessment?
  - Will the firm accept some risk, or will all items be remediated to the extent possible?

Performing Risk Assessments

Risk Assessment Methods

- There are several methods

Establishing Risk

Now we are moving on to the Third phase: Measuring Risk

Measuring Risk

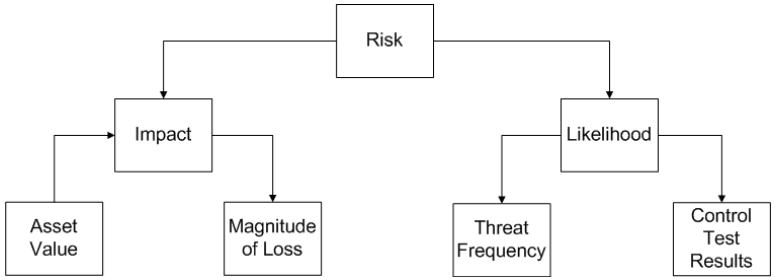
- There are many ways to measure risk, however we will discuss three today:
  - Quantitative – Mathematical Calculations
  - Qualitative – Based on reason
  - Combination – Middle of the road
- The discussion on which method is best is a judgment placed upon organizations to decide. The combination between the two is ideal for a cost effective framework to ensure the appropriate factors are taken into consideration for risk ratings.

Measuring Risk

Risk Methodology

Establish consistent risk rating recommendations and reduce the time spent determining ratings	Ability to consolidate findings into usable and actionable formats	Ensure appropriate factors are considered (Following Slides include these factors)	Asset Valuation (Not necessarily financial)	Ability to substantiate risk determinations to regulatory bodies and audits

Measuring Risk



Establishing Risk

The final discussion today is regarding treatment of Risk.

Remediate / Reduce / Accept

Once risk scoring is finalized

- Remediate / Reduce / Accept

Procedures:

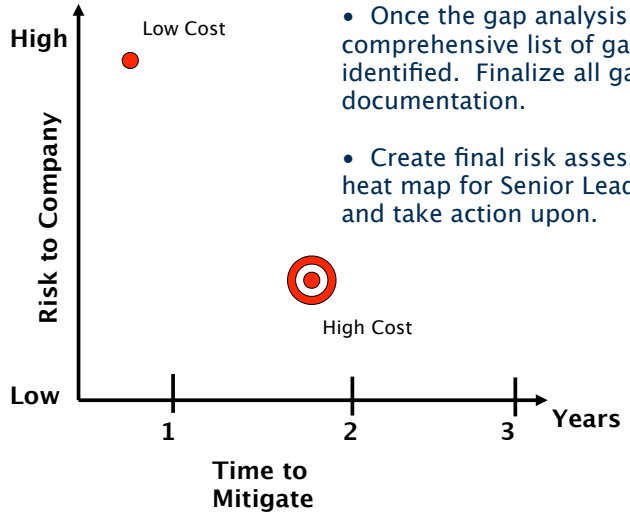
- Budgets, risks, and risk tolerance will all play a role

Remediate / Reduce / Accept

Procedures cont.

- Once risk tolerance has been determined,

Remediate / Reduce / Accept



- Once the gap analysis is complete, a comprehensive list of gaps will be identified. Finalize all gap analysis documentation.
- Create final risk assessment report with heat map for Senior Leadership to review and take action upon.

☒Remediate / Reduce / Accept

Projects

- Once expectations have been

- Remediate / Reduce / Accept

Projects Cont.

- Projects should work with business

- Remediate / Reduce / Accept

Remediation Plans should include the following items to

☒Remediate / Reduce / Accept

Tools

- Any number of tools can be used for remediation

Establishing Risk

Questions?