Sarbanes_Oxley Act 2002

Internal Control Reporting Requirements

Overview of Act

- CEOs and CFOs are required to certify
  - Financial disclosures are complete and accurate,
  - "Disclosure controls and procedures" are in place to ensure reporting of material.
- Which Companies?
  - Publicly traded companies – "Issuer" of stock.

What Should Companies do?

- Response should encompass at the minimum the following:
  - An independent and qualified audit committee of the board of directors
  - Immediate reporting of trades in the company's securities by insiders (within 2 days)
  - Fully documented and certified internal controls and procedures on disclosure
  - Auditability of compliance with these controls

Internal Control?

- Requires the management to file an "Internal Control" report with the annual report.
  - Responsibilities to establish and maintain internal control and procedures of financial reporting
  - Report on Effectiveness of these procedures
- Can reduce "Regulatory Risk" by well-documented and monitored controls and processes.

Internal Control Components

- Control Environment
- Risk Assessment
- Control Activities:
  - Policies and procedures to ensures that polices are enforces
- Information and Communication
  - Processes and systems to
    - Identify, capture and exchange information
- Monitoring
  - Determine Performance of Control processes over time

Controls

- Transactions are properly authorized
- Assets are safeguarded against improper use
- Transaction are properly recorded and reported.

Where can Technology Help?

- Very difficult to control internal processes manually.
- Need electronic checks and balances.
- Need a centralized “policy” control.
- Need a centralized “recording” of all activity.
- Need a centralized “auditing” facility.
- Need a centralized control of “work flow”.

Policy

- Roles and privileges.
- Identification of risks
- Identification of privileges
- Role is a set of privileges
- Assign Roles to Individuals

Work Flow

- Need Dynamic control over the processes
- Should be able to modify the work flow dynamic in response to an atack.