Jeff Reich

Chief Security Officer,

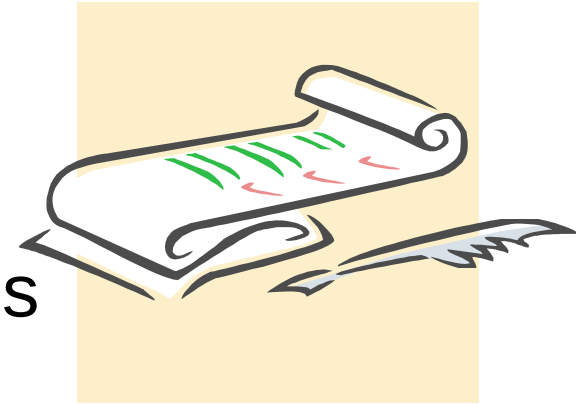
Rackspace Managed Hosting

Session Abstract

When you were first faced with the reality of compliance, you spent your time dealing with and interpreting the various regulations, and may have even brought in auditors to help with this often daunting task. Today, the realization is that compliance is an ongoing process that you must tie to your risk management strategy. But how much is all this going to cost? In this session, Jeff Reich, Chief Security Officer - Rackspace Managed Hosting, shows you what has worked for him at different companies and how such solutions could play out for you in terms of: ...

Topics

- How to Determine Your Risk
- Risk Management
- Know Your Business
- Regulatory Threat Vectors
-
- Use Standards as Tools
- The Correct Level of Compliance Makes
- Manage the Risk with Compliance in Mind



- I was asked to present a case study…

Case Closed

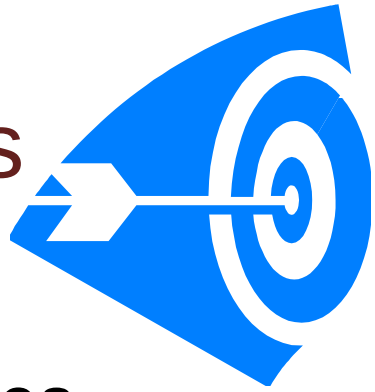
- I performed an exhaustive case study

- x Vulnerability x Cost
  - *Threat* is the frequency of potentially adverse events. Since threat (by this definition) is always a frequency, it's always potentially measurable.
  - *Vulnerability* is the likelihood of success of a particular threat category against a particular organization.
  - *Cost* is the total cost of the impact of a particular threat experienced by a vulnerable target.

Risk Management

- Enterprise Risk Management - Integrated Framework
  - COSO Created an Executive Summary in September 2004
  - http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf
  - You can take any combination of these activities on any Risk:
    - Accept
    - Assign
    - Mitigate
    - Transfer

Know Your Business



- Determine what your enterprise does
- Be able to represent your enterprise to the press
  - What is your "*elevator pitch*?"
- Determine your key business drivers
- If it is not important to your enterprise, it is not important to you
- Determine the cost of compliance

- Laws, Regulations and other impositions
  - Auditors
  - Examiners
  - Oversight
  - $ Fines

- Standards, Policies and Agreements
  - Contracts
  - Self-Assessments
  - Business Partner Audits
  - Public Perception

with:

- Key Business Leaders
- Finance Department
- Internal Auditors
- External Auditors
- Regulators
- Examiners
- Operators
- Who else?

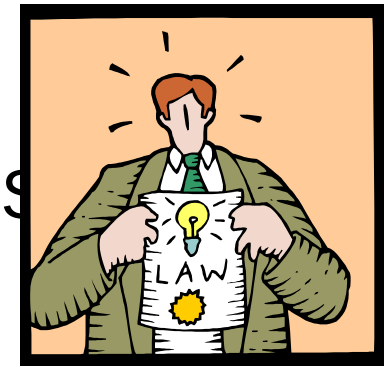
Laundry List

- Sarbanes-Oxley Act
- Gramm-Leach-Bliley Act
- Health Insurance Portability and Accountability Act (HIPAA)
- USA PATRIOT Act
- Office of Foreign Assets Control Regulations
- Office of the Superintendent of Financial Institutions Regulations
- US Federal Rules of Civil Procedure

Even More Laundry

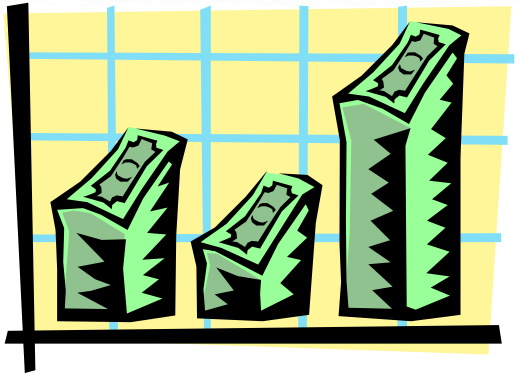
- Occupational Safety & Health

  (OSHA)
- International, Federal, State and Local Regulations
- Industry Standards
- Payment Card Industry Data S
  Standards
- Basel II



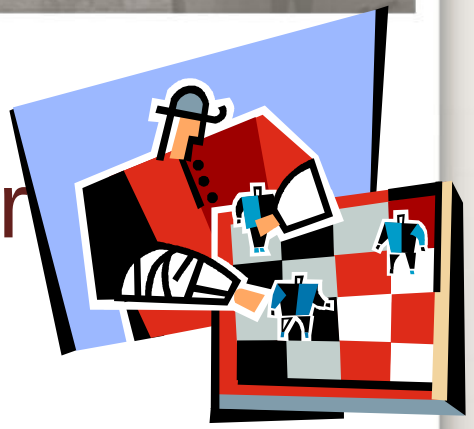
E-Discovery

- Federal Rules of Civil Procedure
  - Electronic Discovery
    - Civil Litigation
    - Metadata
    - Raw Data
      - Bates Numbering System
  - Document Coding
  - Conveniences vs. Standard Document Coding
  - Email Archiving



- For the results, not the reason
  - Compliance should be the result of a good controls program
  - Not be the reason for the program
- If you attempt to achieve compliance only, you will:
  - Spend more money than you need to
  - Never be caught up with rules and regulations
  - Probably not be as secure as you need to be

Governance and Contr



- Compliance can only be achieved and sustained with governance and controls
- Compliance audits look at your results and your processes
- Processes must have inherent controls
- It all goes back to basic security measures for a foundation

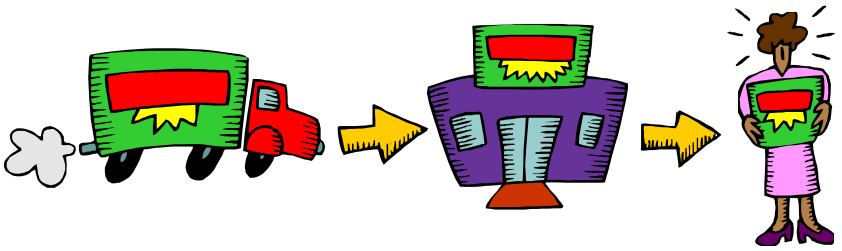
- Use standards to help you achieve your objectives, where applicable
- Avoid using standards as your only measure of success
- Use the appropriate s to be determined by you

Statement on Auditing Standards No. 70 (SAS70)

- Type I report
  - Whether the service organization's description of its controls presents fairly, relevant aspects of the controls that had been placed in operation as of a specific date
  - Whether the controls were suitably designed to achieve specified control objectives.
- Type II report
  - Same items noted above in a Type I report
  - Whether the controls that were tested were operating with sufficient effectiveness to provide reasonable assurance that the control objectives were achieved
- http://www.sas70.com/

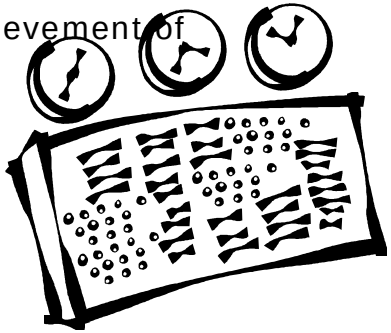
Information and related CobiT)

-
  - IT process and control framework linking IT to business requirements
  - Now used more frequently as a framework for IT governance
  - Current version is CobiT 4.1
- http://www.isaca.org



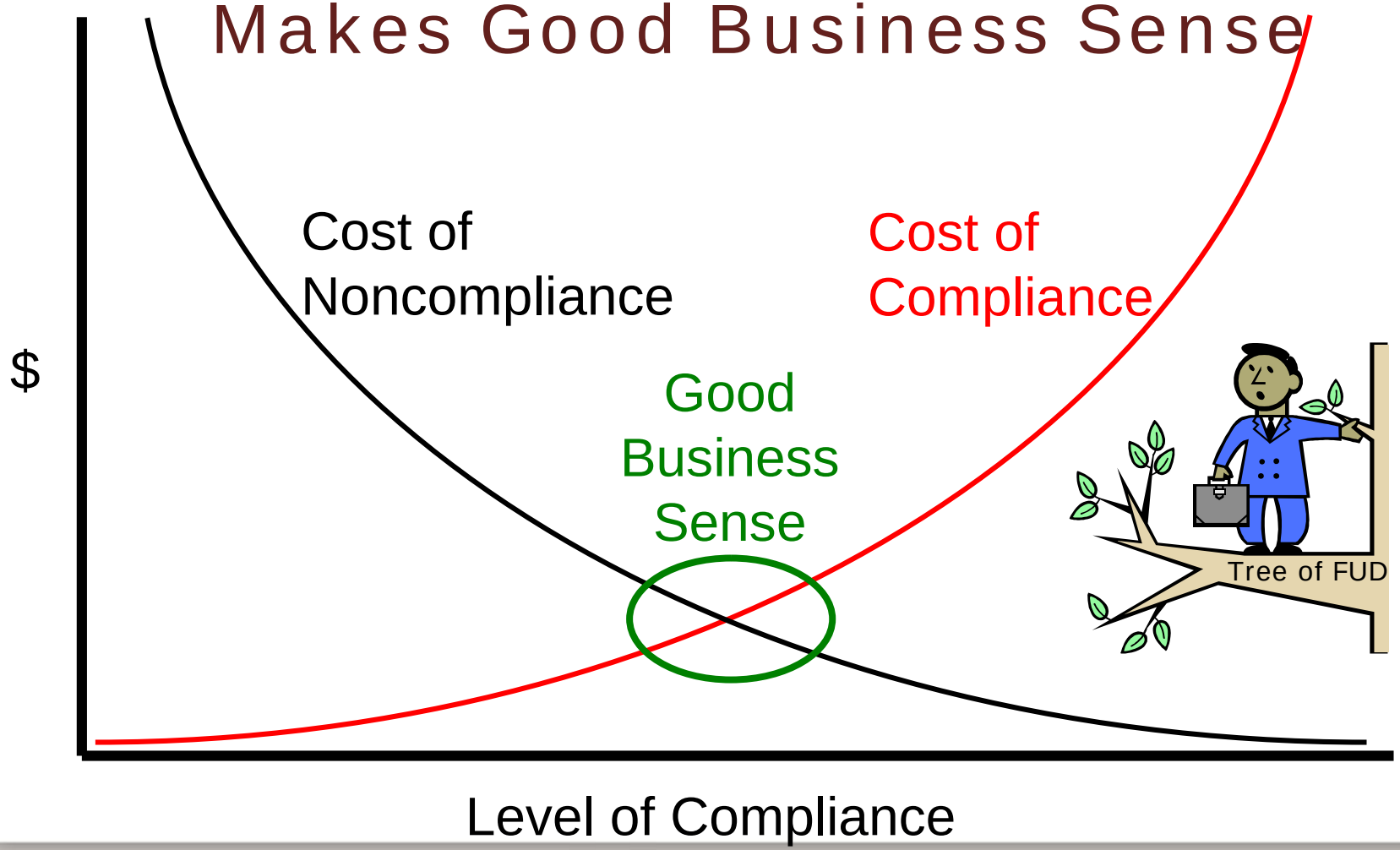
The Committee of Sponsoring Organizations of the Treadway

- A genetic predecessor to Sarbanes Oxley Act
- COSO Definition of Internal Control
  - A process designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
    - Effectiveness and efficiency of operations
    - Reliability of financial reporting
    - Compliance with applicable laws and regulations



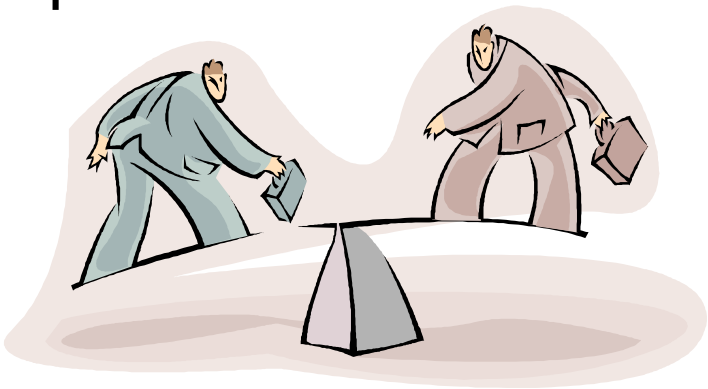
- Internal Control
  - Is a *process*
  - Is effected by *people*.
  - Can be expected to provide only *reasonable assurance*
  - Is geared to the achievement of *objectives* in one or more separate but overlapping categories.
- http://www.coso.org

The Correct Level of Compliance Makes Good Business Sense



in Mind

- Manage risk according to your business
- Your risk profile needs to include both sides of compliance
- Obtain buy-in from your partners
- Periodically re-assess
  - Quarterly
  - Semi-annually
  - Annually
- Enjoy the benefits



Want to find me?

Jeff Reich

jeff.reich@rackspace.com

210-312-3217