Regain Control of IT Compliance Costs through Process Improvement

John Bryer
Practice Director, Health Insurance Solutions
Anexinet

Where Leading Edge Technology Meets Competitive Advantage

Agenda

- Sarbanes-Oxley Overview
- Compliance and Controls
- SOX for Private Companies?
- Common Frameworks – COBIT, COSO, ITIL
- Examples of Effective Controls
- 8 Ways That You Can Take Control

Sarbanes-Oxley (SOX) Act of 2002

- **Section 404** deals with *Management Assessment of Internal Controls*
- SOX requires that Management **document, control, and secure processes that have bearing on reported financial results**.
- No compliance "checklist" ~ each company's risk profile is unique
- SOX typically involves four phases: **PLAN**, **REMEDIATE**, **TEST**, **SUSTAIN**

Compliance and Controls

Compliance - Being in accord with their Rules of some Authority

In Simplest Terms - You're on your way to compliance if an objective 3rd party (external auditor) believes that:

- Your Rules (Controls) are appropriate, given your organization's unique risks
- Your Rules are in accord with the Authority's rules (SOX 404)
- Your Rules are adhered to, as demonstrated by *Evidential Matter*

“My company is private. Compliance doesn’t apply to me”

- Private *Application Service Provider* (ASP) whose service is relevant to a public company’s financial reporting
- ASP may need to demonstrate that systems and processes are sufficiently controlled
- SAS 70 Type II audit “Statement on Auditing Standards No. 70” demonstrates that ASP offers a *consistent, reliable and secure operating environment*

“My company is private and I’m not an ASP. Compliance *still* doesn’t apply to me.”

- A private company’s ability to demonstrate effective control has competitive benefit and can enhance customer satisfaction and retention.
- When selecting (public) vendor who has relevance to your financial reporting see if they have a SAS70
- Even if the service they are to provide has nothing to do with your financial reporting, it’s a way to gain insight into potential vendors

"My company is private, I'm not an ASP, and I don't use vendors. Compliance *still* doesn't apply to me."

- Even organizations that don't need to be "compliant" need to be in control**...**
- **...** even Mario Andretti's racing team:

"If things seem under control, you are just not going fast enough."

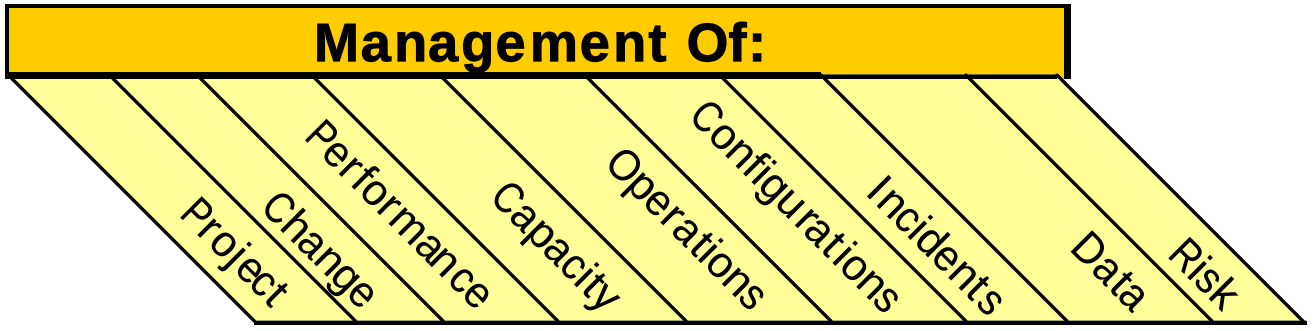
– Mario Andretti

- All organizations have some Controls in place (SLAs, metrics, policies)
- Are your controls part of cohesive, business-aligned governance?
- If controls don't encourage strong business alignment, you're missing the big payoff (because that ultimately increases technology ROI)

Even if they don't recognize it as "compliance" all IT organizations are involved in control activities

Does your IT organization engage in any of the following?

Control Activities
Direction setting: Technology, Strategy, Investment
Technology: Acquisition, Implementation, Management
Information Technology: Processes, Organizations, Relationships
Security
Cost Allocation
Training

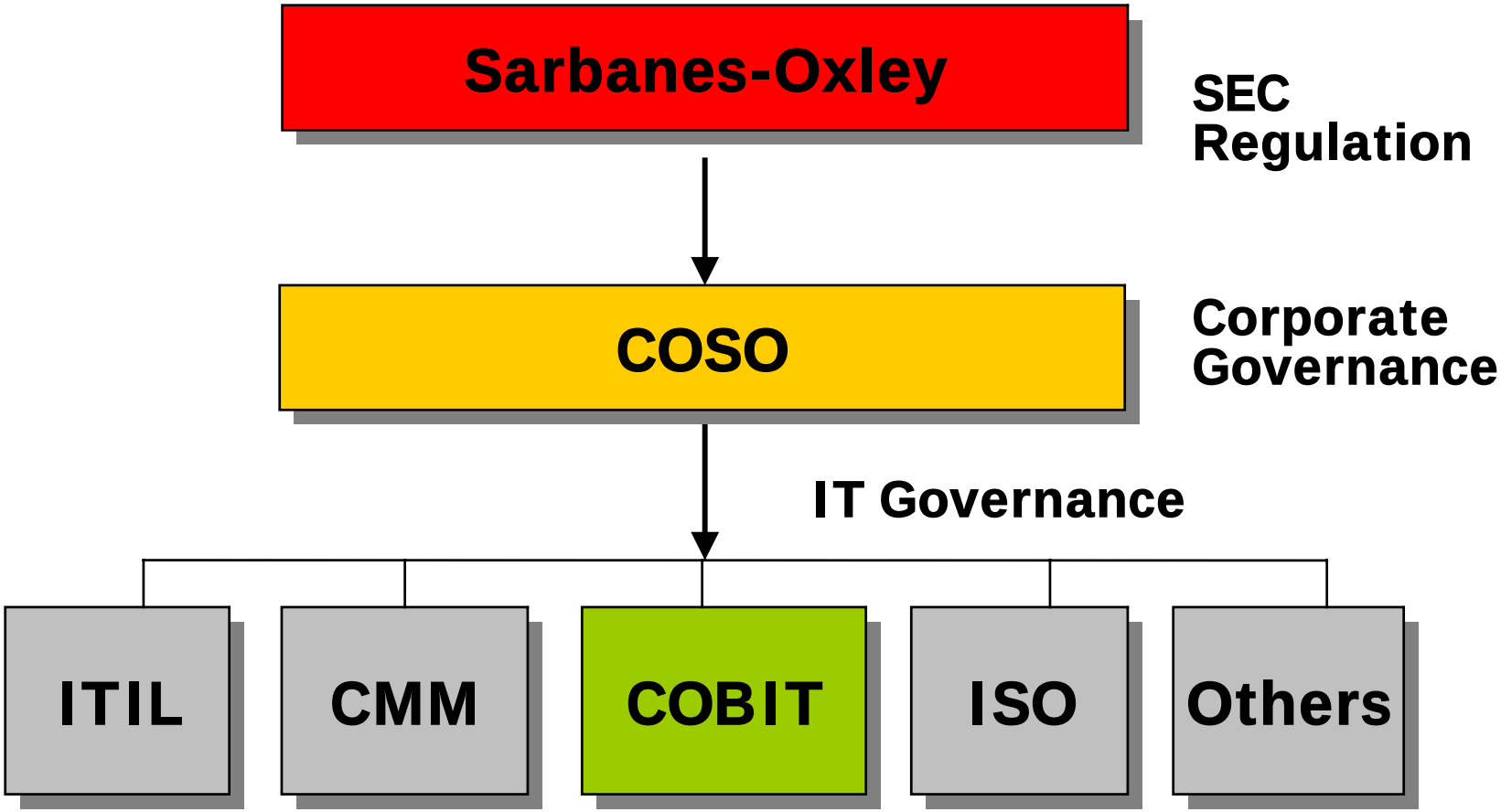


We've just summarized the 34 high level COBIT control objectives

Agenda

- Sarbanes-Oxley Overview
- Compliance and Controls
- SOX for Private Companies?
- Common Frameworks – COBIT, COSO, ITIL
- Examples of Effective Controls
- 8 Ways That You Can Take Control

Common Frameworks – COSO, COBIT & ITIL



COSO – The Committee Of Sponsoring Organizations of the Treadway Commission

- Key concept: **internal control is a process that depends upon people at every level of the organization**
- Control objectives are intended to provide reasonable assurance regarding:
  - operational effectiveness and efficiency
  - reliability of financial reporting
  - compliance with applicable laws and regulations
- **COSO**'s target audience is management at large; **COBIT** focuses more on IT

COBIT - Control OBjectives for Information and related Technology

- COBIT is best described as ***IT governance with a clear business focus*** that fulfills COSO requirements for the IT control environment
- COBIT-based IT governance focuses on the following areas:
  - Strategic alignment of business and IT
  - Ensuring that IT delivers the promised benefits
  - Resource management (processes, people, apps, systems, and information)
  - Risk management
  - Performance measurement

ITIL - Information Technology Infrastructure Library

- Focuses on **IT services**
- Often used to complement the **COBIT framework**
- Detailed comprehensive **set of management procedures**
- **Customizable framework** of best practices
- Owned by United Kingdom Government's *Office of Government Commerce*
- Consists of 8 "sets" of documents:

ITIL®
IT Service Management

1) Service Support discipline
2) Service/Help Desk discipline
3) Security Management
4) The Business Perspective
5) Planning to Implement Service Mgt
6) ICT Infrastructure Management
7) Applications Management
8) Software Asset Management

Agenda

- Sarbanes-Oxley Overview
- Compliance and Controls
- SOX for Private Companies?
- Common Frameworks – COBIT, COSO, ITIL
- Examples of Effective Controls
- 8 Ways That You Can Take Control

Example of Controlling a Process - “Improper account provisioning with segregation of duties”

Simple scenario:

- A manager ask system admin for user account for new employee.
- The admin knows the person making the request; grants access.
- Approval is implied; accountability is ambiguous.

Problematic from a Control perspective:

- Poor separation of responsibilities: REQUEST, APPROVE, IMPLEMENT
- Does policy permit this type of employee to have this access?
- Accountability is ambiguous
- No evidential matter for internal and external audit to test

Example of Controlling a Process - "Improper account provisioning with segregation of duties"

How to Get Control of the Process

1. Recognize that improperly controlled granting of access is a risk area.
2. Craft policy defining acceptable system access by employee position.
3. Define who can *request*, *approve*, and *implement* access.
4. Implement controls to ensure that the policy is being adhered to.
5. Educate all affected employees about the policy and the control.

Remediated Process:

- Requestor documents the Request
- Approver documents that they approve the Request
- Implementation occurs
- Implementer documents that the Implementation occurred
- Auditors examine all documentation and ensure coherence with policy

More Examples of Insufficient Separation of Duties

A/R

A/P

Changes to code

Deploy to production

Example of Change Control While Generating Savings - "Insufficient controls for change management"

Situation:

- Public company had 20 SOX 404-critical financial spreadsheets
- 80% of organizations use Excel in some form to do financial reporting
- Spreadsheets resided on user's PCs and were manually maintained

Risks:

- No versioning
- Prone to errors
- No consistent back-ups
- Conflicting results across spreadsheets
- Company wanted to address 404 risk and reduce expenses

Example, continued…

Costs:

- Reports were run to collect information (1.5 hrs/ss)
- Information from the reports was entered into spreadsheet (1.5 hrs/ss)
- Spreadsheet calculations were run and verified (2 hrs/ss)
- Resolve any discrepancies (0-4 hrs/ss)
- Results communicated to management
- Total annual cost for 20 spreadsheets: **$168,000**

Solution:

- Spreadsheets moved to central servers
- Microsoft Visual Studio Tools for Office (VSTO) used to greatly improve control of the process
- VSTO provides users with a familiar Excel tool set
- User Interface provides an action pane to control data management

Example, continued…

Benefits (Phase 1 of 4):

- Greatly reduced 404 risk
- Spreadsheets now being secured
- Spreadsheets backed up
- Spreadsheets maintained
- Data inconsistencies addressed

Cost savings:

- Solution (Phase 1 of 4)
- Management runs reports directly
- Lengthiest run time reduced to 20 seconds
- Cost estimated to be $80,000/year
- Savings in Year 1: **$88,000**
- Savings in Year 2+: **$168,000**

Agenda

- Sarbanes-Oxley Overview
- Compliance and Controls
- SOX for Private Companies?
- Common Frameworks – COBIT, COSO, ITIL
- Examples of Effective Controls
- 8 Ways That You Can Take Control

8 Ways That You Can Take Control

1) *Get help and build positive relationships*

- Essential to engage the services of an experienced SOX partner
  - External auditors are careful to not provide SOX consulting
- Develop positive relationships
  - Among company, a SOX partner and the external auditor
  - Between IT and the business

2) *Get control by giving control*

- Require the business to play active role
- Alleviates uneasiness about technology cost
- Helps fight perceptions of IT unresponsiveness and non-alignment

8 Ways That You Can Take Control

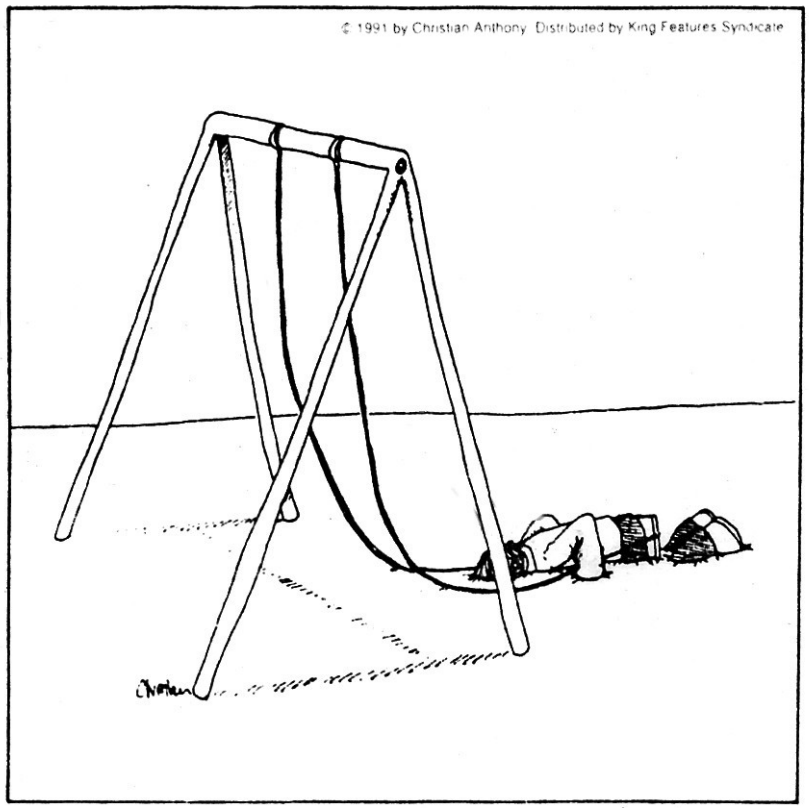
3) IT Steering Committee - a good way to keep the business engaged

- The most direct way to foster **IT-business alignment**
- CIO as facilitator of discussion about discretionary IT resource expenditures
- Maintain business support by frequent re-evaluation of business alignment
- Avoid old perceptions of IT dictating
- **Demystifies IT**

8 Ways That You Can Take Control

4) *Make sure control environment is designed correctly and that everyone is on board*

- "Obtain management commitment."
- "Assess entity-level 'tone-at-the-top' controls early in the process.'"
- Executive "tone" has huge impact on control internalization

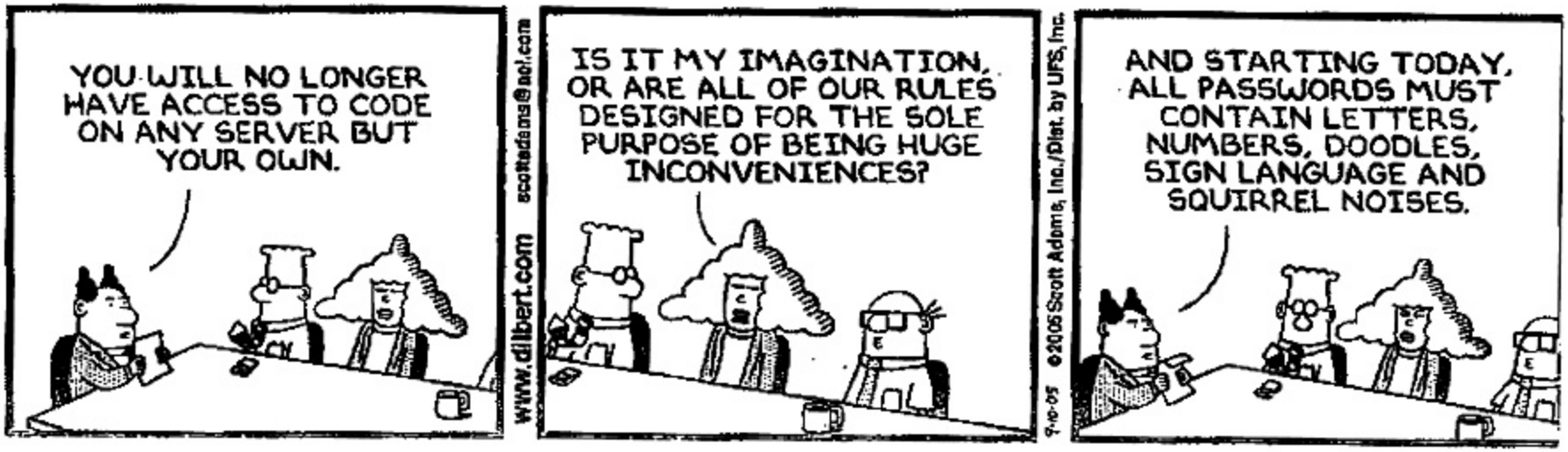


Poor design.

8 Ways That You Can Take Control

5) *Build support across the organization*

- Allow input from those affected by it; need their strong buy-in
- Controls are most effective if based on clearly understood policy
- Broad understanding of the need for a control reduces resistance
- Educate affected population to understand that controls are not arbitrary



8 Ways That You Can Take Control

6) *Look for ways to control cost and to reap benefit from investments*

- Determine if external auditors will use results of 3rd party testing:
  - Saves on external audit expense.
  - Advances testing of controls to earlier in the process.
  - Raises audit concerns earlier in the process when there is still time to remediate
- Rely on automated tools
  - Need a cohesive, end-to-end control infrastructure
  - Automate request/approve/implement workflows
  - Provide evidential matter
  - Reduces day-to-day interruptions

8 Ways That You Can Take Control

7) Get control through knowledge and understanding

- You can't control what you can't measure.
- Process documentation helps clarify R&R
- Documentation that results aids new employees, reduces dependency others
- Project lifecycle standardization:
    - Helps clarify and finalize requirements earlier it the process
    - Enables project comparisons for prioritization
    - Yields efficient resource utilization

8) Manage and test control processes

- Frequent testing to ensure controls are working
- If evidential matter isn't being created, the control isn't working

In Summary

Benefits of Control:

- Decrease Costs
  - Improves the efficiency of resource consumption (“Never time to do it right; always time to do it twice”)
- Increase Revenue
  - Improves customer satisfaction
  - Improves customer (and investor, and auditor) confidence.
- Improve Quality
  - The process discipline will allow clarification of Requirements earlier in the development process
  - Promotes better IT-business alignment (e.g., IT Steering Committee)

Thank You

Contact Information:

John Bryer, Practice Director, Health Insurance Solutions

jbryer@anexinet.com

#484-686-3763