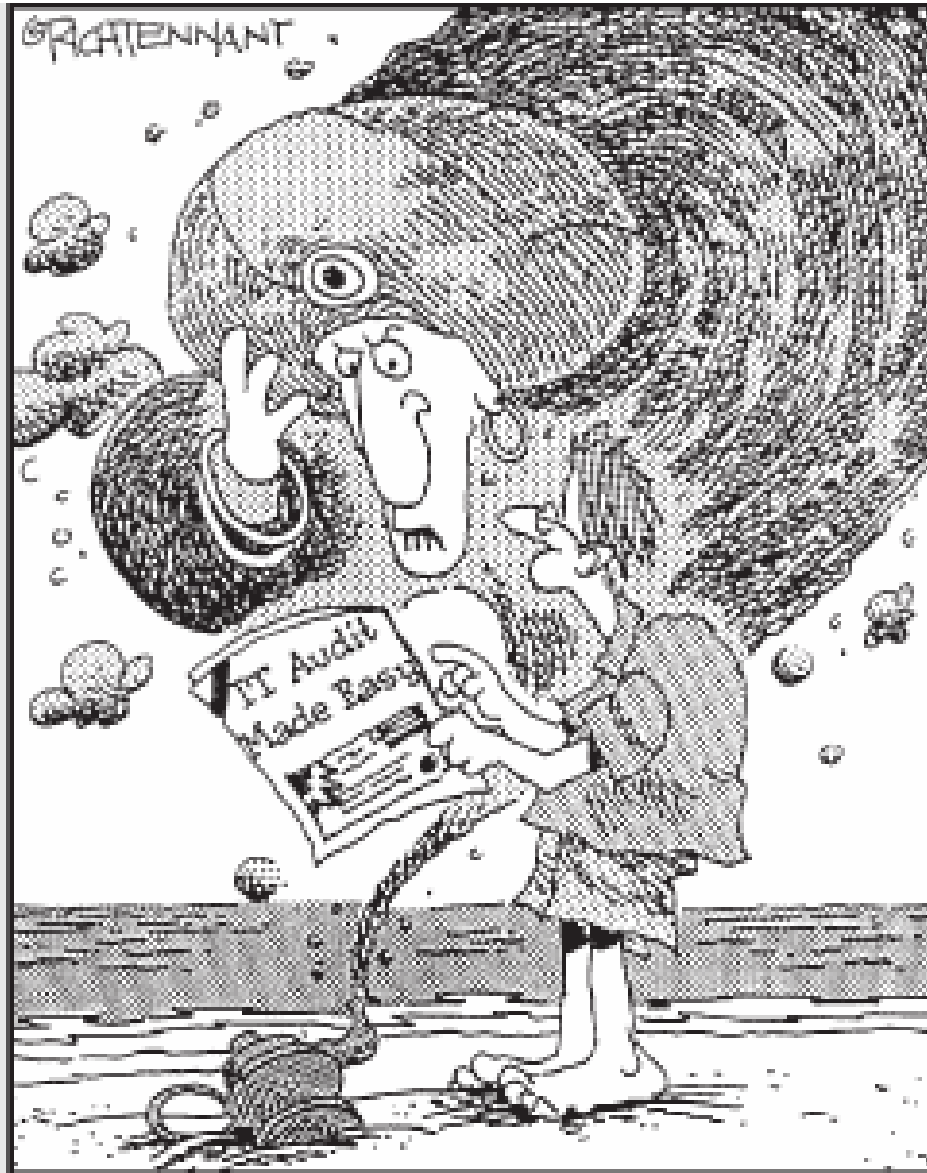


Sustainable IT Compliance

Observations and Directions

David Greene
Active Reasoning
September 14, 2005



"Can't I just give you riches or something?"

Sustainable IT Compliance

“The dirty little secret of the first Sarbanes-Oxley audit is that no one really knew what they were doing. Not the auditors, not the consultants, not you.”

– “How to Dig Out From Under Sarbanes-Oxley”, CIO Magazine, 7/1/2005

- Where Are We Today?
- Sustainable IT Compliance
- Reduce IT Controls
- Close the Loop on Change Management
- Automate Compliance Testing
- Common IT Control Deficiencies
- Building on Compliance

Where are We Today? Generally Successful ...

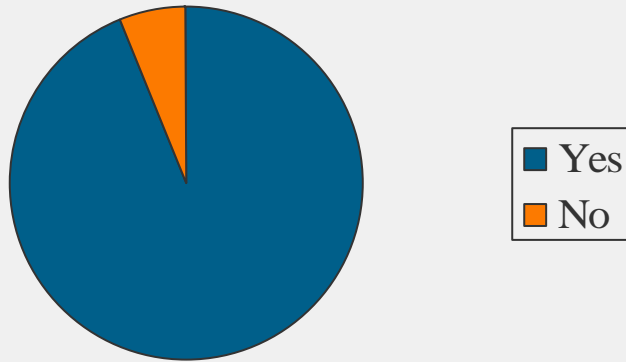


BY INDUSTRY	10-Ks Filed	Passed		Failed	
Automotive & Transport	58	54	93.10%	4	6.90%
Business Services	258	219	84.88%	39	15.12%
Consumer Products Manufacturers	83	73	87.95%	10	12.05%
Electronics	168	145	86.31%	23	13.69%
Energy & Utilities	131	119	90.84%	12	9.16%
Financial Services	344	316	91.86%	28	8.14%
Food & Beverage	28	28	100.00%	0	0.00%
Health Care	92	88	95.65%	4	4.35%
Industrial Manufacturing	117	105	89.74%	12	10.26%
Insurance	98	92	93.88%	6	6.12%
Leisure	28	25	89.29%	3	10.71%
Media	63	55	87.30%	8	12.70%
Pharmaceuticals	149	141	94.63%	8	5.37%
Retail	147	119	80.95%	28	19.05%
All Companies	2033	1823	89.70%	210	10.30%

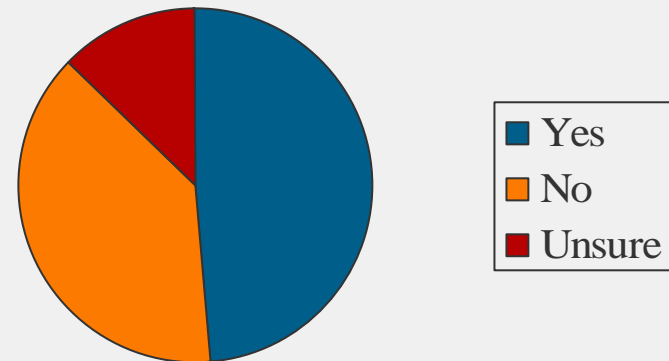
Source: Compliance Week Internal Control Report Card, 8/2/05

... A Few Surprises ...

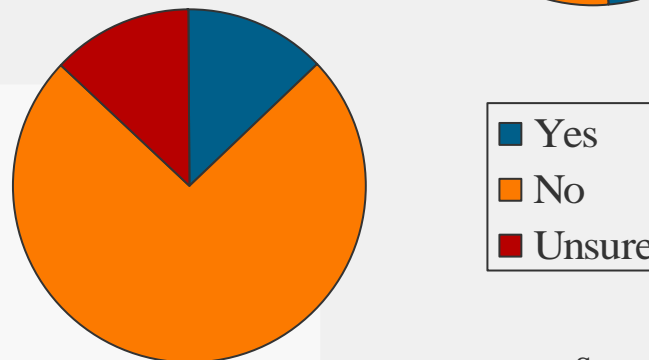
During your Section 404 audit, were any failures/deficiencies attributed to IT?



Have IT issues proved to be a larger part of overall compliance efforts than you company anticipated?



Do you feel that regulators have clearly communicated what constitutes IT controls?



Source: CFO-IT survey of 153 senior executives, Summer 2005

... at an Enormous Cost ...

CIO Perspective

CIO Executive Council Poll, 8/3/2005

- “CIOs estimate their organizations have spent just under **2% of gross revenue** to comply with Sarbanes-Oxley and an average of **\$1,450,000 of their information technology (IT) budget** during the past twelve months.”

Auditor Perspective

Study by Foley & Lardner, 6/05.

- Average audit costs for S&P500 companies **increased 55%** over 2003
- Average audit costs for companies with revenues under \$1 billion **increased 96%**
- Average audit costs for companies with revenues over \$1 billion **increased 56%**

CEO / CFO Perspective

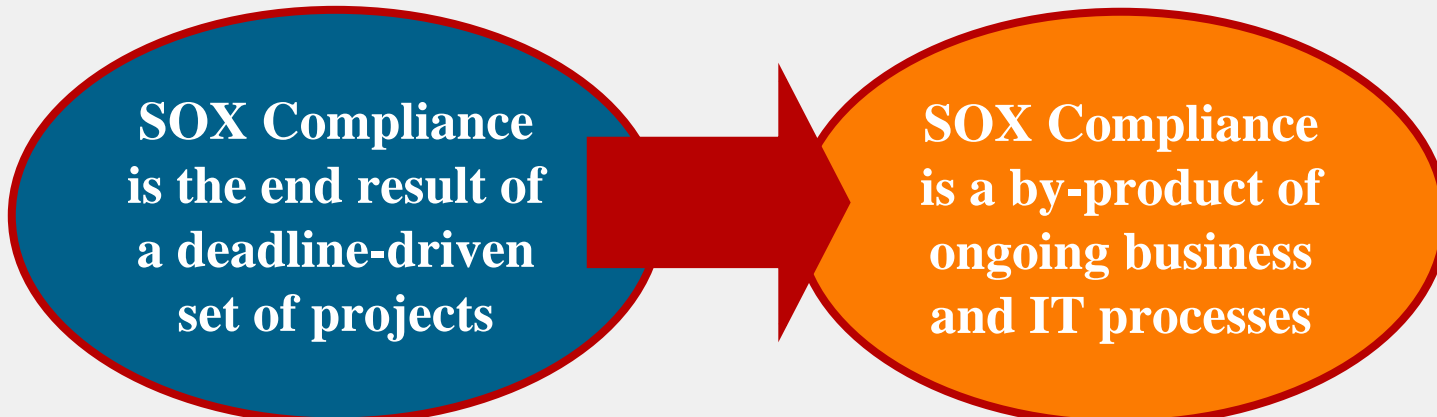
NASDAQ Issuer Survey Sarbanes Oxley Act of 2002, 4/13/2005

- NASDAQ issuers spent an average of **\$1.1 million on Section 404 implementation**
- NASDAQ issuers in total spent an estimated **\$3.5 billion on 404 implementation**
- As a percent of revenue **smaller issuers spent approximately 11 times more** than larger companies

... that is Not Going Away

- **70%** of surveyed CIOs believe that year 2 compliance **costs will either increase or stay the same** – *CIO Executive Council Poll, 8/3/2005*
- “...second-year fees for 404 work will probably come in at about **70 percent of first-year** fees. But all major firms continue to **raise their hourly rates.**” – “*Fractured Fraternity*”, *CFO Magazine, 9/1/2005*
- “FEI [Financial Executives International] surveys indicate that the Sarbanes-Oxley audit represents **57 percent of all audit fees.**” – *Gartner Group, “IT Executive's Best Practice Guide to Sarbanes-Oxley”, 8/31/2005*
- “According to a recent survey commissioned by the largest U.S. accounting firms, auditors believe that the total costs of compliance with Section 404 will **decline by 46 percent next year.**” – *PCAOB Release No. 2005-009, 5/16/2005*

Sustainable IT Compliance



**SOX Compliance
is the end result of
a deadline-driven
set of projects**

**SOX Compliance
is a by-product of
ongoing business
and IT processes**

Invest in the business, not the auditors

- Required compliance activities are long-standing best practices
- How can compliance be a catalyst for making important initiatives urgent initiatives?
- How can current processes and projects be extended to meet compliance requirements?
- How do we manage compliance as a dynamic, evolving, ongoing process?

Strategies for Sustainability

1. Reduce IT Controls

Reduce the complexity and effort of compliance by streamlining your control activities.

2. Close the Loop on Change Management

Extend existing change management processes to meet the expanded requirements of IT compliance.

3. Automate Compliance Testing

Reduce the manual burden and complexity of testing, starting with the “easy win” of automating data collection.

4. Focus on Common Deficiencies

Invest in the weaknesses reported by others – expect these to be the focus of auditor attention regardless of your past performance.

Reduce IT Controls

Too Little Guidance

- “Adversarial” relationship with Auditors
- No clear direction on what was expected by the auditor
- No clear feedback on what was proposed by the company
- Sequential “best guessing.” Internal Audit defines what they believe auditors want to see. IT Audit then defines what they think internal audit wants to see

Too Many Controls

- Most organizations implemented too many IT controls as part of the 2004 audit – “you won’t fail an audit for having too many controls”
- When in doubt implement additional controls
- Results in double burden of implementing the control and proving that it is being used even if it is unnecessary

PCAOB - a New Ally

May 16 2005 Policy Statement

- *Integrate their audits* of internal control with their audits of the client's financial statements, *so that evidence gathered and tests conducted in the context of either audit contribute to completion of both audits*;
- *Exercise judgment to tailor their audit plans to the risks facing individual audit clients*, instead of using standardized "checklists" that may not reflect an allocation of audit work weighted toward high-risk areas (and weighted against unnecessary audit focus in low-risk areas);
- *Use a top-down approach* that begins with company-level controls, to identify for further testing only those accounts and processes that are, in fact, relevant to internal control over financial reporting, and *use the risk assessment required by the standard* to eliminate from further consideration those accounts that have only a remote likelihood of containing a material misstatement;
- Take advantage of the significant flexibility that the standard allows to *use the work of others*
- *Engage in direct and timely communication with audit clients* when those clients seek auditors' views on accounting or internal control issues before those clients make their own decisions on such issues, implement internal control processes under consideration, or finalize financial reports.

Refining IT Controls: Pause and Reassess

Re-Assess Risks and Potential Impacts

- For each defined control, how could a violation of that control result in a material misstatement of financial results?
- What is the likelihood of the control violation occurring?

Consider potential for material impact and potential risk by:

- Application
- Business Process
- Location / Subsidiary

Objectives are to:

- Eliminate redundant or unnecessary controls
- Bound required controls to the relevant infrastructure

Refining IT Controls: Define your Framework

COBIT - IT Control Objectives for Sarbanes-Oxley

- Common starting point for many organizations and auditors
- Well documented and understood
- Excellent starting point for defining IT controls
- May be excessive for some organizations
- Some redundancy
- Useful to reference controls back to standard

	COSO Component				
	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring
COBIT Control Objectives					
Plan and Organize					
Define a strategic IT plan		•		•	•
Define the information architecture			•	•	
Determine technological direction					
Define the IT organization and relationships	•			•	
Manage the IT investment					
Communicate management aims and direction	•			•	•
Manage human resources	•			•	
Ensure compliance with external requirements			•	•	•
Assess risks		•			
Manage projects					
Manage quality	•		•	•	•
Acquire and Implement					
Identify automated solutions					
Acquired and maintain application software			•		
Acquired and maintain technology infrastructure			•		
Develop and maintain procedures			•	•	
Install and accredit systems			•		
Manage changes			•		•
Deliver and Support					
Define and manage service levels	•		•		•
Manage third-party services	•	•	•		•
Manage performance and capacity	•		•		
Ensure continuous services	•		•		•
Ensure systems security	•		•	•	•
Identify and allocate costs					
Educate and train users	•			•	
Assist and advise customers					
Manage the configuration	•		•	•	
Manage problems and incidents			•	•	•
Manage data			•	•	
Manage facilities			•		
Manage operations			•	•	
Monitor and Evaluate					
Monitor the processes				•	•
Assess internal control adequacy					•
Obtain independent assurance	•				•
Provide for independent audit					•

Refining IT Controls: Define your Framework

Common Controls Categories

Aggregated based on feedback from different auditors and their clients

- Application Controls (transaction centric)
- Application Development (SDLC)
- Change Management Controls
- Access Controls (application, systems, database)
- IT Operations
- Backup / Recovery
- Network Security
- Physical Security
- IT Governance

Refining IT Controls: Review with Your Auditor

- Review and request feedback on your proposed control framework
- Be prepared to share the results of your risk assessment and show why the proposed controls are sufficient for the identified risks
- You are the expert on your business and your business processes – not your auditor
- Make this an ongoing process

“In many cases, compliance with Sarbanes-Oxley or other regulations ends up being a negotiation of sorts with your auditor (or other attesting/certifying party). The end result of this negotiation should be an agreement that strikes a balance between meeting the letter and intent of a regulation (or its interpretation) and doing what's most appropriate for your organization....”

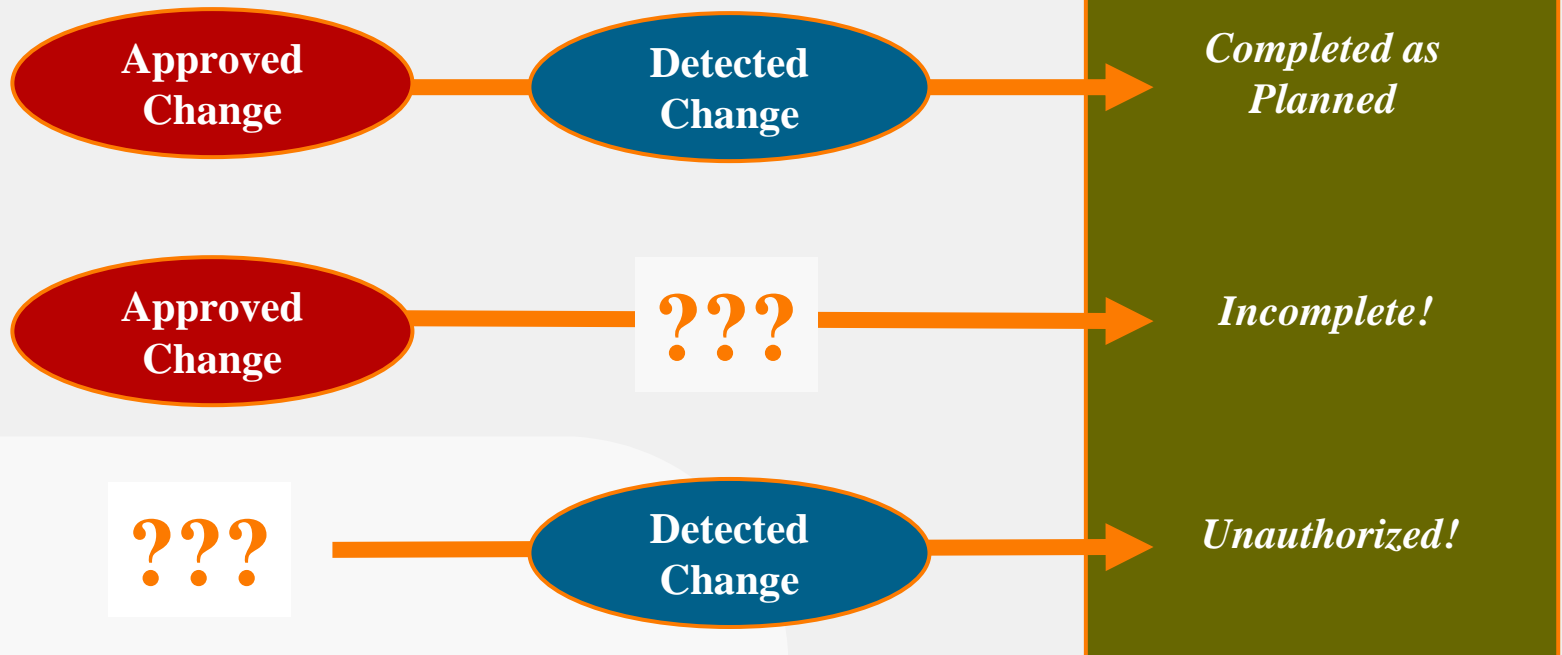
– *“Use Best Practices to Negotiate Sarbanes-Oxley Compliance With Auditors”, Gartner Group, 8/17/2005*

Closing the Loop on Change Management

Planned Activity

Actual Activity

Result



Sample Change Management Control Activities



System changes (both application and infrastructure) are properly authorized, tested, and approved by management

1. The principal analyst or supervisor for an application and the change control board approve all changes before being implemented into production.
2. Version control is maintained as items are moved into the production environment.
3. System modifications are prioritized based upon criticality, cost and timing dependencies with related modifications based upon the input from business users.
4. Segregation of duties exists among testing, approving, and executing changes.
5. User review/acceptance testing is performed before changes are made to production.
6. A test environment exists in which program changes can be thoroughly checked for errors and modified as needed.
7. Once a system change is made, all of the appropriate system documentation is updated to reflect the change.

Current Change Management

Existing mature Change Management processes and tools can be the foundation for Change Management compliance controls

- Well defined change management process, preferably based on ITIL Change Management processes
 -] Process includes formal definition of what constitutes “approved change”
 -] Process can accommodate emergency changes
- Change Management process applied broadly across the IT infrastructure, at a minimum to all critical SOX applications and supporting technologies
- Implemented using change management software, such as solutions from Remedy, Peregrine, or HP Service Desk. Preferably one and only one change management system in use
- Process is applied proactively on an ongoing basis, not documented after the fact

Current Change Management Assessment

- Do we have an effective change management process?
- What controls are in place in our change management process?
- Have we seen benefits from the change management process?
- Remember that site-wide outage we had last week because of a change? What happened?
- What process was used to determine the cause of the outage?
- How does IT monitor the health of the process?
- What is the goal of our change management process?
- How disruptive is our patching process?

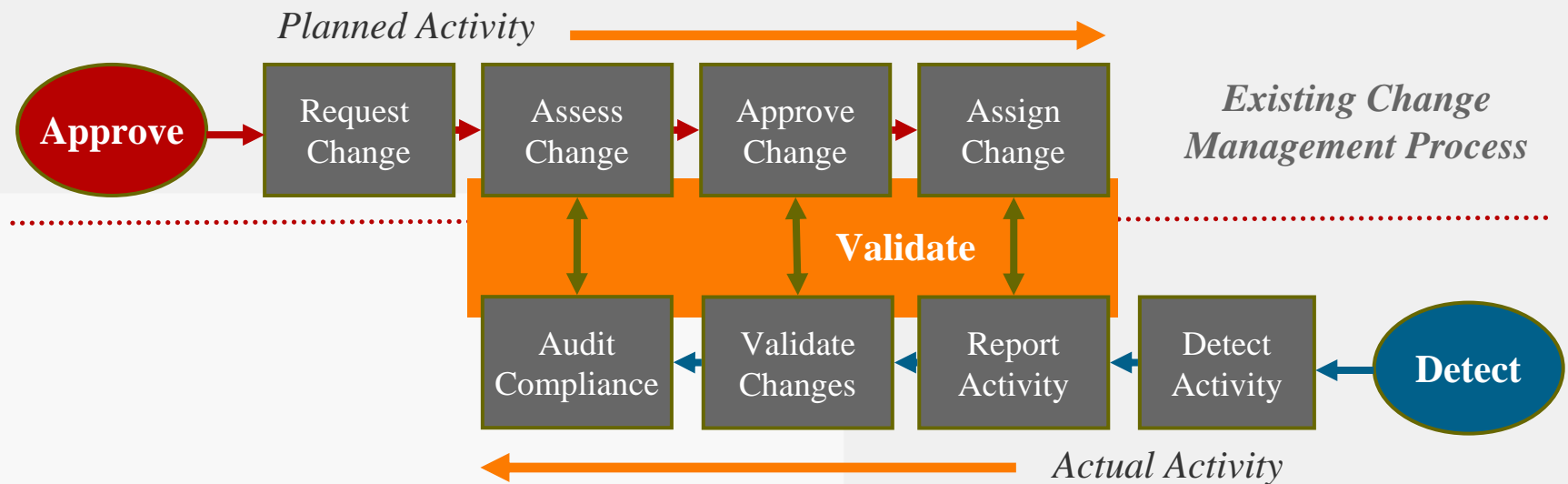
“...organizations with better IT change and patch management processes require fewer system administrators. When IT change and patch management work well, IT personnel are more effective and productive.”

– “Global Technology Audit Guides v3.1 Change and Patch Management Controls: Critical for Organizational Success”, Institute of Internal Auditors 3/11/2005

Change Validation

Approve, Detect, and Validate IT Change

- Existing change management process and systems used to request and approve changes
- Change detection processes and systems used to capture actual activity
- Change validation used to compare actual activity to approved activity



Change Validation Approaches

Exact Match

Validate change based on exact match of every observed activity to expected changes

- Requires up-front definition of all change details usually down to the file / database table level
- Gives absolute certainty of validation
- Impractical for most organizations

Example: A change request specifies that four configuration files will be changed. Jack makes changes in five files. Change is considered unauthorized.

Attribute Match Inference

Validate change based on key attributes of observed activities

- May include consideration of such attributes as assigned user, time of change, target application, and target system.
- For many classes of changes offers sufficient level of control for audit purposes

Example: Jack was assigned a change request to update the order processing system with a new software release. Changes were made by Jack to one or more application files during the time and on the system identified in the change request. Jack actions are considered authorized.

Extending Current Change Management Process

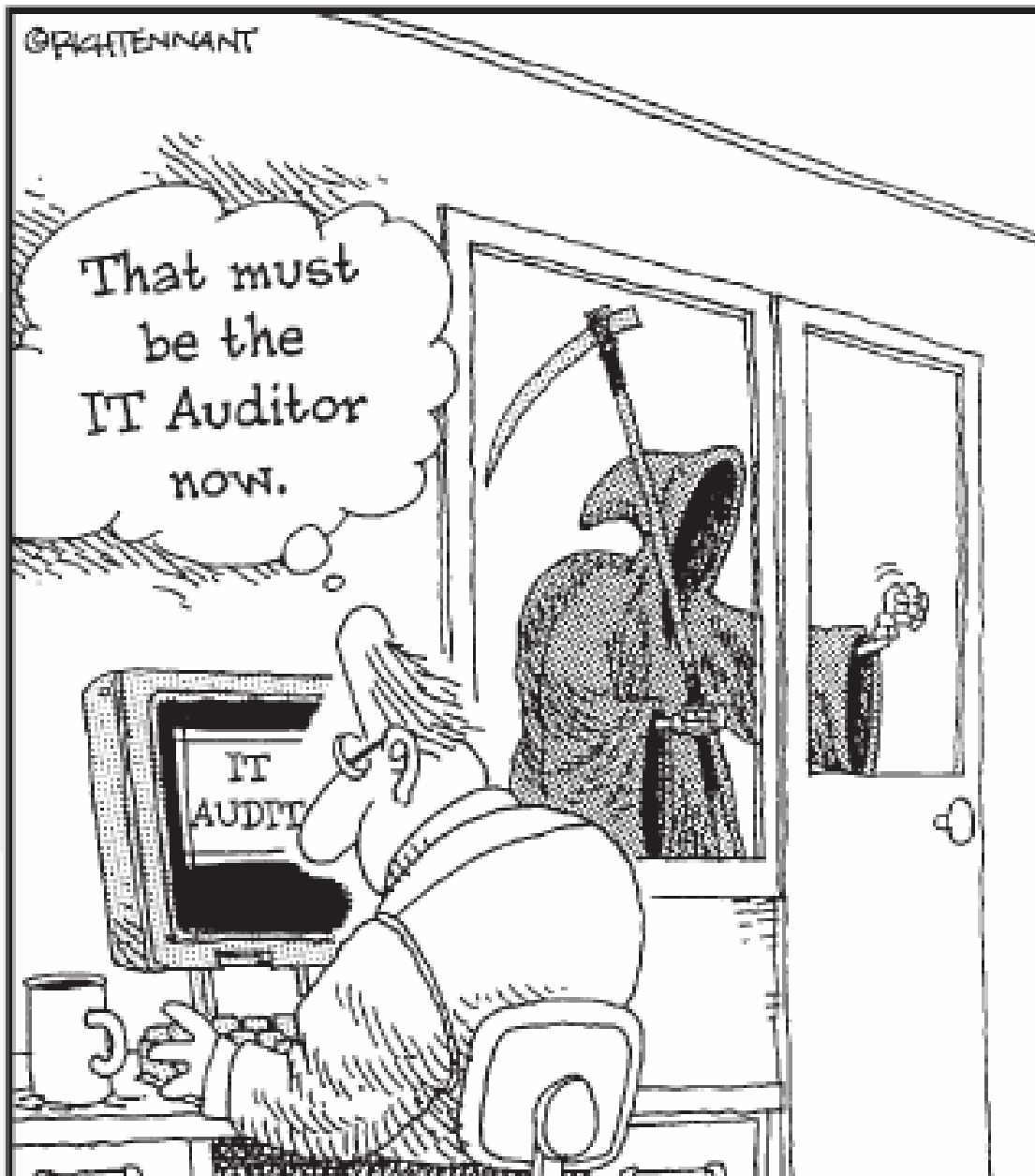


Control

- A. Changes approved before release to production environment
- B. Segregation of duties between requesting, approving, and executing functions
- C. Changes are prioritized
- D. User review / acceptance testing before changes are made to production
- E. System documentation
- F. Expected / staged / requested version is released into production
- G. Test environment for each application

Validation Procedure

- A. Use Attribute Matching to compare approved change request to detected activity.
- B. Requestor and Approver already tracked by change management. Supplement with executor of observed actions
- C. Prioritization can be required for approval of change request. Use "A" to detect un-prioritized (unauthorized) changes.
- D. User acceptance can be required for approval of change request. Use "A" to detect un-prioritized (unauthorized) changes
- E. Requires a manual control.
- F. Maintain archive copies of version file / table. Compare to change request.
- G. Track overall usage of test environment



Automating Compliance Testing

2004: Manual Testing

- Focus on raw data collection and manual review
 -] Keyboard logging followed by review
 -] Reassigned team to review system logs
 -] Daily review of change requests against system

Key Challenges

- Labor intensive
- No guarantee of completeness
- Test of detailed examples is not the same as a test of the process

Testing Sampling Standards

Manual Controls

Validation sample size

- Annual Controls – 1
- Quarterly Controls – 2
- Monthly Controls – 2 to 5
- Weekly Controls – 5 to 15
- Daily Controls – 20 to 40
- Control used multiple times per day – 25 to 60
- More critical controls use higher end of these ranges

Automated Controls

1

- Testing one item may be sufficient
- Focus on override policies and procedures

Source: PricewaterhouseCoopers, Sarbanes-Oxley Act:
Section 404 – Practical Guidance for Management, 7/2004

Automated Data Collection

Application: Vantage Tax
 Start Time: 01-11-05 14:00
 End Time: 01-11-05 16:00

Time	Device	Type	Name	Event	User	Action
01-11-05 14:00:04	UTYHQCOMET	Process	cmd.exe	Started	bbackus	Approved
01-11-05 14:23:16	UTYHQCOMET	File	c:\win32\programs\vantage\ config.data	Modified	bbackus	Approved
01-11-05 14:46:11	UTYHQCOMET	Process	cmd.exe	Stopped	bbackus	Approved
01-11-05 14:52:20	Oracle_01	Application Internal	sales_region_data	Modified	ggorman	Violation

Application: General Ledger
 Start Time: 01-11-05 14:00
 End Time: 01-11-05 16:00

Time	Device	Type	Name	Event	User	Action
01-11-05 14:10:28	GL_HQ_01	File	/QSYS.LIB/CRMSPGM.LIB /RSXJDFR#.FILE	Modified	ftillman	Violation
01-11-05 14:24:11	SAP_01	Process	cmd.exe	Stopped	bbackus	Approved
01-11-05 14:25:02	SAP_01	File	c:\win32\programs\vantage\ config.data	Modified	bbackus	Approved
01-11-05 14:25:58	SAP_01	Process	cmd.exe	Stopped	bbackus	Approved
01-11-05 14:36:24	SAP_01	Process	notepad.exe	Started	awalsh	Approved
01-11-05 14:37:01	SAP_01	File	d:\SAP\GLbackup\back.log	Modify	awalsh	Approved
01-11-05 14:38:08	SAP_01	Process	notepad.exe	Stopped	awalsh	Approved

Automated Reporting

Data Presentation

Collection is only half of the battle

- System generated reports for auditors – no manual manipulation
- Interactive reporting for investigation
- Multiple views – by application, by control, by business function

Other Applications

Consider other ways to leverage this data

- Problem / incident management
- Forensic review
- Operations monitoring

Common IT Control Deficiencies

Have You Heard the One About...

Same IT control deficiencies are appearing again and again

-] Across auditors
-] Across companies
-] Across industries

More to Come Next Year

Expect future audits to focus proportionally greater attention on these deficiencies

-] Generally correspond to “high risk” controls
-] Auditors know more than they did last year
-] Growing body of knowledge and expertise on these areas

Focusing on these deficiencies can have the biggest impact on compliance success and effectiveness

SOX “Greatest Hits” IT Control Deficiencies

Excessive Access to Systems / Databases

- Developer / programmer access to production environment
- Developer / programmer access to production data
- DBA access
- System Administrator access

Lack of Access Controls

- User provisioning and administration
 -] Changes in responsibilities
 -] Changes in organization
 -] Terminations
- No documented access policies and standards
- General monitoring of the security infrastructure

SOX “Greatest Hits” IT Control Deficiencies

Improper Change Management

- Lack of formal program change procedure
- Lack of understanding of system configurations
- Oversight of changes and review of change logs

Insufficient Segregation of Duties

- Separation of requestor, approver, implementer
- Separation of developers and operators

Lack of Self Assessment

- Late implementation of controls
- Failure to identify abnormal application transactions
- Failure to consider automated controls
- Ongoing testing program

Building on IT Compliance

How Can You Use IT Compliance To ...?

- Improve IT operations
- Improve change control
- Improve uptime
- Increase accountability
- Reallocate resources through automation
- Reduce operations costs
- Improve security
- Improve your overall compliance score
- Attain closer alignment of IT and the business
- Gain competitive advantage

Additional Information

David Greene

-] Vice President of Marketing and Professional Services
-] david.greene@activeresaoning.com
-] 650 404 9904

Peter Lipovsek

-] District Sales Manager
-] peter.lipovsesk@activereasoning.com
-] 614 761 8661

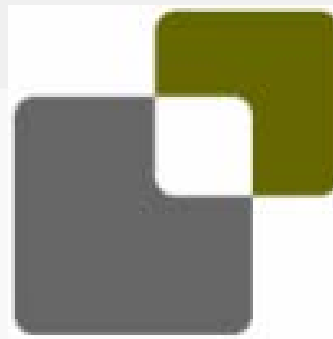
You are welcome to share this presentation with others who may find it useful

Active Reasoning

Active Reasoning develops automated change audit solutions that *identify and reduce unauthorized changes and uncontrolled access* to the IT infrastructure.

- Focus on people's actions – who, what, when, where
- Reduce the cost and effort of ongoing testing and validation of compliance controls
- Ensure that all changes, even unauthorized changes, are detected and reported
- Improve ongoing operations and uptime

Actual Activity
What really happened?



Planned Activity
What was supposed to happen?



Compliance for People Who Mean Business™

www.activereasoning.com