

# Improving Recommendations in IT Audits

---

Arthur Foreman CISA, CISSP  
Jesse Hanford, CISA

Greater Cincinnati ISACA  
Monthly Meeting  
4 January 2011

# The lawyers would like you to know...

The thoughts, viewpoints, and statements of this presentation are those of the presenters only, and are not necessarily those of Convergys Corporation, or its affiliates.

This presentation is based purely on personal experience and research. Any official viewpoints implied or stated are purely coincidental.

Art's statements may also be whimsical.

So there!

# The challenges of 2011...

No Budget



No Time



Not Enough Staff



# And one more...

Critical projects of the year have just re-prioritized everything, leaving the organization at risk.



# Topics for Discussion

- Definition, purpose, scope of recommendations
- Characteristics of good recommendations
- Using standards and expert opinions
- Causal analyses
- More suggestions for getting action on recommendations
- Examples

# Definition, Purpose, Scope of Recommendations

- Definition
  - ◆ Auditors' suggestions of what management should do to improve reportable problems AND
  - ◆ Management's agreed upon actions
- Purpose
  - ◆ Mitigate reoccurrence of the problems identified in the findings
  - ◆ Show audit report reader that auditors don't only focus on the past
  - ◆ Formerly, a method of selling consulting services

# Definition, Purpose, Scope of Recommendations (Continued)

- Scope
  - ◆ Operational auditing (IT auditing)
  - ◆ System oriented
- Endorsed
  - ◆ IIA's Practice Advisory 2410, Communication Criteria
  - ◆ ISACA recommended
  - ◆ Government Auditing Standards (7.21-3)



# Characteristics of Good Recommendations

- Useful and appropriate
  - ◆ Address findings
  - ◆ Related to root cause of problem
  - ◆ Cost-effective
  - ◆ Doable and workable
  - ◆ Not overly specific
  - ◆ Timely
  - ◆ Acceptable to management (normally)
  - ◆ Understandable

# Characteristics of Good Recommendations (Continued)

- Recommendations need support in the work papers
  - ◆ IIA Standard 420
  - ◆ Work papers should include
    - ☞ Management agreement
    - ☞ Research showing basis of recommendation
    - ☞ Make it seem like a compliance audit
    - ☞ Causal analyses to show significance

# Using standards and expert opinions

- Advantages
  - ◆ Sanctioned
  - ◆ Already debated
- Sources
  - ◆ COBIT
  - ◆ ISO27000
  - ◆ Payment Card Industry standard
  - ◆ NIST SP800-53 (Recommended) and FIPS 200 (Required)
  - ◆ ITIL

# Using causal analyses

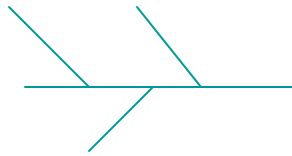
- Advantages
  - ◆ Accepted quality control techniques
  - ◆ Looks scientific
  - ◆ Shows significance
- Examples
  - ◆ Ishikawa (fishbone)
  - ◆ Pareto
  - ◆ ISO
  - ◆ Six Sigma

# Using causal analyses (Continued)

## ■ Example – Not fixing vulnerabilities

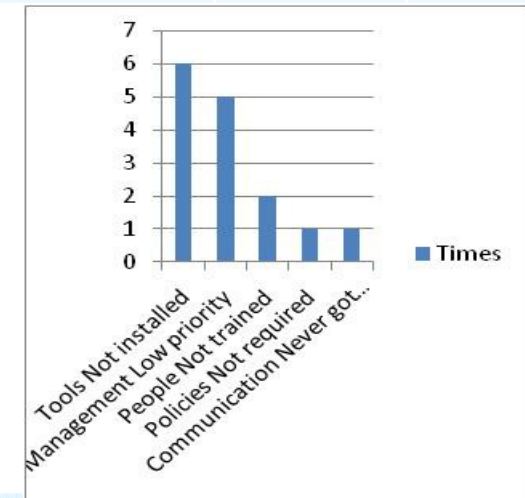
### ◆ Causes by reason

### ◆ Ishikawa (fishbone)



### ◆ Pareto

Cause Class	Cause	Times
People	Not trained	2
Management	Low priority	5
Policies	Not required	1
Tools	Not installed	6
Communication	Never got info	1
unknown		3
no problem		4



# How do we combat these items?

- Start with your documented IT Standards and Policies as your baseline...you do have this right?
- Make sure you have executive buy-in or sponsorship.
- Involve the IT Governance Department.
- Leverage existing resources to get the job done.
- Use milestones to break large tasks into smaller units.
- Follow-up is imperative, otherwise...

# The Risk of Abandonment Increases



# Goofus and Gallant as Auditors

- **Goofus Recommends:** An enterprise change detection tool should be procured, configured, and implemented to detect unauthorized changes to the production environment. To be completed 6 months from audit report issuance.
- **Gallant Recommends:** In the short term, a monthly control should be implemented in conjunction with development and production personnel to manually compare production libraries with known changes. In the long term, software solutions including existing software packages should be evaluated as an automated control in the detection of unauthorized changes. Short term to be completed 1 month from audit issuance, with the long term evaluation results to be completed 6 months from the audit report.

# A history lesson...

Legacy Systems can teach us a lot about modern IT audit recommendations



# Examples

- Unapproved programs running
  - ◆ By [date], computer operations or some independent group outside of the application development group monitor activities in the production processing environment to detect the execution of programs (e.g., jobs) by programmers (ISACA P-10)

# Examples (Continued)

- Testing with real and private data without secured environment
  - ◆ test managers must begin reviewing data by [date] to assure the data is simulated and/or by [date] require tester to adhere to security controls for real data



# Examples (Continued)

- Encryption keys easily compromised due to no key management procedures
  - ◆ determine if more extensive key management procedures (including key creation, key protection, and re-keying) are needed and, if so, create and implement them... **(bad)**



# Examples (Continued)

- Terminated, transferred, and deceased individuals have active accounts
  - ◆ security administration review re-confirm access based on the ISO-27000 standard 17799 (9.2.4) beginning [by date], reassign accounts that cannot be removed, and require technical management to review installation of all software to assure software runs out of a system account ... (bad)



# Examples (Continued)

- Updates for unused computer software is being purchased and time is wasted updating the software
  - ◆ technology must install usage counter for all purchased computer software [by date]. Purchasing must have approval from technology to buy updates to any software....



# Summary

- Make sure recommendations are specific, address finding, effective, relate to finding's root cause, **cost-effective**, workable, timely, and understandable
- Documented basis of recommendation in work papers with managerial agreement



# Go Forth and Recommend

- May all your recommendations be acceptable unto IT management