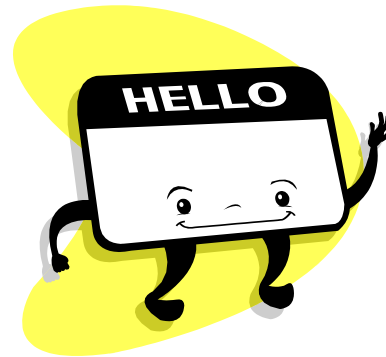


Writing an Audit Finding

Danny M. Goldberg

**Professional Development Practice
Director**

I. Introduction





Danny M. Goldberg

- Professional Development Practice Director, Sunera
(www.sunera.com)
- Founding Partner, SOFT GRC
(www.thesoftaudit.com)
- Former Director of Corporate Audit/SOX at Dr Pepper Snapple Group & Tyler Technologies
- Established/Assisted in Establishing 3 Internal Audit/SOX Departments over the past 6 years
- Texas A&M University – 97/98
- Father of two beautiful kids!



Danny M. Goldberg (cont.)

- CPA – Since 2000
- CIA – Since 2008
- CISA – Since 2008
- CGEIT (Certification in the Governance of Enterprise IT) – Since 2009
- CCSA (Certification in Control Self-Assessment) – Since 2007
- Served on the Audit Committee of the Dallas Independent School District
- Board Member – American Lung Association Dallas Chapter
- Published Author
 - *Internal Auditor* Articles (April & December 2007)
 - *ISACA Online* Article – December 2009
 - June 2010 – *Audit Report* – Cover Article – “How the Recession is Changing is Internal Audit”
 - October 2010 *Internal Auditor* – *CAE’s as A/C Members: It Just Makes Sense*
 - December 2010 *New Perspectives* - *Sell Your Work: How to Deliver Best Practice Audit Reports*
 - Book Publication in Fall 2010 – *Internal Audit: Fundamental Principles and Best Practices* – www.bna.com
 - January 2011 – *Dallas Business Journal* – *The Yes Man Phenomenon*

Sunera Snapshot



- ✓ **Professional consultancy** focused on regulatory compliance, internal audit, information technology & accounting advisory services
- ✓ Founded by former public accounting partners and professionals
- ✓ Delivered more than **1200 projects** to over **300 clients** across a broad spectrum of industries
- ✓ Employ **100+ full-time professionals** in **eleven offices** across the United States and Canada
- ✓ **PCI** Qualified Security Assessor (**QSA**) & Approved Scanning Vendor (**ASV**)
- ✓ **Registered with NASBA to offer CPE's** for our ACL & Internal Audit training courses
- ✓ **Certified integration partner** for leading continuous controls monitoring solutions, including **ACL, Approva & SAP**

Our Values

Thought Leaders

We deliver **proactive, unbiased**, tried and true **guidance**.

Quality

We deploy **fulltime, trained** and **certified professionals** with appropriate oversight utilizing proven, pragmatic **methodologies** to ensure our teams deliver **consistent results**. Our professionals are accustomed to working together using standardized approaches and delivery methods resulting in a unified engagement team.

Collaborative

We **tailor each project** to your specific needs. Our **flexible, client-centric** approach enables us to deploy teams which complement our clients' internal capabilities, address resource constraints and facilitate knowledge transfer.

Responsive

We readily adhere to **your timetable**, unlike “Big-4” firms which are burdened by onerous internal risk management practices and busy season restrictions.

Solution Focused

We are known for completing projects that **achieve anticipated benefits, on-time** and **within budget**. Our rigorous project management discipline combined with our finance and IT capabilities enables us to successfully deliver a wide-range of services.

Balanced Perspective

We recognize that “best practices” are not always appropriate and provide cost-effective solutions that find the right **balance between risk and control**.

Sunera Offices



Professional Development Clients



THE BATON ROUGE CHAPTER



THE BIRMINGHAM CHAPTER

THE PITTSBURGH CHAPTER

THE ALBUQUERQUE CHAPTER



TEXAS SOCIETY OF CERTIFIED PUBLIC ACCOUNTANTS



BlueCross BlueShield of North Carolina

THE FOX VALLEY / CENTRAL WISCONSIN CHAPTER



FWIIA.ORG

THE FORT WORTH CHAPTER OF THE INSTITUTE OF INTERNAL AUDITORS



HoustonIIA.ORG

THE HOUSTON CHAPTER OF THE INSTITUTE OF INTERNAL AUDITORS



The Association for Accountants and Financial Professionals in Business

III. Audit Report Structure

Contents of a Typical Audit Report

- Executive Summary
- Observations
- Appendices

Contents of a Typical Audit Report

- Observations
 - Criteria
 - Condition
 - Cause
 - Effect
 - Recommendations
 - Action plans

Observation Components



Observation Components

- Foundation
- Condition
- Cause
- Effect
- Recommendations
- Action plans

Foundation

- It is what we are measuring against
- 3 types of Foundation:
 - Internal: Company's policies and procedures
 - External: Regulatory/legal mandates
 - Best-Practice: Expectations in the company/industry & general research on the best way to do things.



Foundation– Continued

- Internal Foundation – Examples
 - Company travel& entertainment policy
 - Internal information, technology, security and access policies
 - Internal Human Resources code of conduct
 - Any policy/procedure in a company
 - Can be an informal process/procedure but formality assists in enforcement

Foundation – Continued

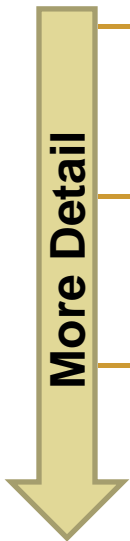
- External Foundation – Examples
 - Government requirements (HIPPA)
 - Sarbanes-Oxley Act of 2002
 - Tax regulations

Foundation – Continued

- Best Practice Foundation – Examples
 - GAAP
 - Segregation of Duties – general best practice
 - 3rd Party Vendor System Guidance
- What are other sources of best practice?

Condition

- Just the facts, ma'am!
- Various levels of detail (dependent on degree of finding and organization)
 - Cruising Altitude Summary – grouping of conditions combined along a commonality – “view from the top”
 - Just after Take Off Summary – conditions are grouped based on commonalities
 - Boarding Summary – individual records and detail; granular detail



Condition - Continued

- What is the right level of detail?
 - Depends on:
 - Your organization and Audit Department's internal standards and Audit Committee requirements
 - Importance of finding (risk rating)
 - Number of issues identified
 - Type of audit
 - Auditee
 - ETC, ETC, ETC.
 - What else?

Group Exercise



EXERCISE– 15 minutes

- Write all 3 types of summaries based on the facts below:
 - » 25 expense reports were selected to review
 - » Audit Step: Verify all were filed in accordance with company policy and within current limitations and standards.
 - » Results: 1 of the sample selected (below) had numerous charges (see attached for detail) that were not appropriately supported by receipts
 - » 1 expense report had duplicate descriptions and totaled exactly \$.01 under the dollar amount necessary for additional approval.

Name	ID #	Date	Amount
Jim Scott	2614	4/12/09	999.99
- Dinner	Travel	4/8/09	75.74
- Red Sox Tickets	Entertainment	4/7/09	209.38
-Dinner	Travel	4/8/09	138.92

Condition

■ Examples:

– Cruising :

- We selected 25 expense reports to review; all were filed in accordance with company policy and within limitations. We noted 1 of the sample selected had charges that were not appropriately supported by receipts.

– Take Off:

- We selected 25 expense reports to review; all were filed in accordance with company policy and within limitations. We noted 1 of the sample selected had charges that were not appropriately supported by receipts and ***totaled exactly \$.01 under the dollar amount necessary for additional approval.***

Condition - Continued

■ Examples:

– Boarding:

- We selected 25 expense reports to review, all of which were filed in accordance with company policy and within current limitations and standards. We noted 1 of the sample selected (Jim Scott) had numerous charges (see attached for detail) that were not appropriately supported by receipts and are duplicate descriptions and totaled exactly \$.01 under the dollar amount necessary for additional approval.

Name	ID #	Date	Amount
Jim Scott	2614	4/12/09	999.99
- Dinner	Travel	4/8/09	75.74
- Red Sox Tickets	Entertainment	4/7/09	209.38
-Dinner	Travel	4/8/09	138.92

Condition: Writing Good Summaries

- Aggregate – use numbers
- Find commonalities
- Use examples
- Don't over-summarize

Cause

- What's the difference?
- 3 Types of cause
 - *Contiguous: the action or lack of action that led directly to the condition*
 - *Transitional (middle): the cause or causes that led to the proximate cause*
 - *Core: underlying cause*

Group Exercise



EXERCISE

- Write each of the three type of causes based on the following facts (condition)
 - 27 employees were asked to verify knowledge of the IT security policy and compliance with the policy.
 - 12 of the sample reviewed were not aware of the policy
 - 5 were not found in compliance with current standards.

Cause - Example

Condition	
Contiguous Cause	
Transitional Cause	
Core Cause	

Cause - Example

Condition	27 Employees were asked to verify knowledge of the IT security policy and compliance with the policy. 12 of the sample reviewed were not aware of the policy and 5 were not found in compliance with current standards.
Contiguous Cause	Employees were not aware of the policy as it was not given to new employees when hired nor was discussed when violations occurred.
Transitional Cause	Human Resources did not have a procedure in place to give the policy to new employees and IT was not aware of the lack of knowledge of the policy when violations occurred.
Core Cause	Communication is limited between Human Resources and IT and thus a lack of communications to employees.

Effect

- Risk or exposure to the company
- Levels of effect
 - *Direct, one-time effect*
 - *Cumulative effect on the process*
 - *Cumulative effect on the organization*
 - *High-level, systematic effect*


Effect – Practice Advisory

■ Standard 2410

- The risk or exposure the organization and/or others encounter because the condition is not consistent with the criteria (the impact of the difference).
- In determining the degree of risk or exposure, consider the effect their engagement observations and recommendations may have on the organization's operations and financial statements.


Effect - Example

<p>Condition</p>	<p>27 Employees were asked to verify knowledge of the IT security policy and compliance with the policy. 12 of the sample reviewed were not aware of the policy and 5 were not found in compliance with current standards.</p>
<p>Direct, one-time effect on the process</p>	
<p>Cumulative effect on the process</p>	
<p>Cumulative effect on the organization</p>	
<p>High-level, systematic effect</p>	



Effect - Example

Condition	27 Employees were asked to verify knowledge of the IT security policy and compliance with the policy. 12 of the sample reviewed were not aware of the policy and 5 were not found in compliance with current standards.
Direct, one-time effect on the process	12 Employees were not aware of the policy thus violate the policy routinely due to the lack of knowledge.
Cumulative effect on the process	The organization does not have an effective IT policy in place due to lack of communication of the policy to employees.
Cumulative effect on the organization	The integrity of the IT control environment is compromised.
High-level, systematic effect	The organization has data integrity issues due to the lack of policy communication.



Recommendations Practice Advisory

- 2007 Practice Advisory – Standard 2410
 - Engagement communications should include:
 - Recommendations for potential improvements
 - Acknowledgments of satisfactory performance
 - Corrective actions
 - Should be based on the internal auditor’s observations and conclusions and call for action to correct existing conditions or improve operations
 - May suggest an approach to correcting or enhancing performance as a guide for management in achieving desired results.
 - Recommendations may be general or specific
 - » Example: under some circumstances, recommendation of a general course of action and specific suggestions for implementation may be desirable . In other circumstances, it may be appropriate only to suggest further investigation or study

Recommendations and Action Plans

- They describe what is to be done
- This is the real substance of the audit report; where auditors can really add value
- Any recommendations and action plans should be discussed and agreed to (if possible) with the auditee prior to report finalization.

Action Plans– Practice Advisory

- 2007 Practice Advisory – Standard 2410
 - As part of the internal auditor’s discussions with the engagement client, the internal auditor should try to obtain agreement on the results of the engagement and on a plan of action to improve operations, as needed.
 - If the internal auditor and engagement client disagree about the engagement results, the engagement communications may state both positions and the reasons for the disagreement.
 - The engagement client's written comments may be included as an appendix to the engagement report.
 - Alternately , the engagement client's views may be presented in the body of the report or in a cover letter.

Types of Recommendations and Action Plans

- **Cause focused** – Address actionable causes; identify and describe what is to be done to prevent recurrences of the condition.
 - Essential for significant or material observations but may not be needed for other, lower-rated observations
- **Condition focused**– address the condition identified and describe what will be done to correct the condition.
 - May not be required; varies from company to company
- **Recovery-focused** – address the consequence of the condition and describe what will be done to correct errors caused by the condition.
 - Not always appropriate based on the condition and may not be required in your company.

Recommendation & Action Plans - Example

<p>Cause-focused recommendation and action plan</p>	<p>Recommendation - Management should enhance communication between Human Resources, Information Technology and Employees to provide the requisite knowledge and understanding on IT Policies and Procedures.</p> <p>Action Plan – The leadership team, including members of HR and IT, should meet at least monthly, to make sure employee training needs are met and reconcile all new employees to verify they have been made aware of requisite IT policies.</p>
<p>Condition-focused recommendations and action plan</p>	<p>Recommendation – Employees should be aware of the requisite IT policies to adhere to them.</p> <p>Action Plan – As part of the new hire checklist, IT policies are given to each new employee and each employee is asked to sign off stating they have read and agree to each.</p>
<p>Recovery-focused recommendation and action plan</p>	<p>Recommendation - Monthly, Human Resources should review all new hire paperwork to verify acknowledgment of policies and IT should, when any incidences are reported, verify knowledge of policies and make training available.</p> <p>Action Plan – Dalton Diedier, HR Manager, is now responsible for performing the reconciliation of new employees monthly. Additionally, IT is being trained on proper communications when incidents occur.</p>

III. Summary

Things to Remember

- Apply the standards but remember they are grey on purpose
- Know your organization
- No surprises!
- Use common sense