The Changing Regulatory Landscape: 
What Internal Audit Needs to do to Get Ready

Lori Turbé
Professional Standards Partner
Grant Thornton LLP
404-475-0200

January 11, 2013
Agenda

- PCAOB Developments
  - Professional Skepticism
  - Observations from 2010 Inspections
- SOC Reports
- COSO Framework
- Foreign Corrupt Practices Act
Learning Objectives

• Gain an understanding of how current PCAOB communications to audit firms will impact the nature and expected documentation of a Company's internal control environment, testing and documentation.

• Recognize high-risk areas and potential flags for FCPA violations, as well as best practices to mitigate those risks
PCAOB Staff Audit Practice Alert No 10
December 4, 2012
Maintaining and Applying Professional Skepticism in Audits
Professional skepticism is an attitude that includes a **questioning mind**, being alert to conditions that may indicate possible misstatement due to fraud or error, and a **critical assessment of audit evidence**.

The alert touches on three main concepts:

1. Why professional skepticism is important
2. Threats to skepticism
3. Safeguards to skepticism
Professional Skepticism

Professional skepticism is especially important for:

- Areas which involve significant management judgment
- Transactions outside the normal course of business
- Areas the auditor considers higher risk

Needs to consider contrary evidence!
Auditors will ask more **why?** questions and anticipate management to have considered:

- Why is 6 months without a sale appropriate for determining inventory reserves?
- Why is a 10% discount rate appropriate?
- Why is over 90 days appropriate?
- Why is 5% growth in your revenue forecast used when it's been 1% in the past?

**Why is your assumption appropriate?**
Professional Skepticism

Specific examples of instances where PCAOB believes professional skepticism could be enhanced:

- hard to value assets – how does Company evaluate
- consideration of subsequent events
- impairments
- reserves
- other key estimates
PCAOB Release No. 2012-006
December 10, 2012
Observations from 2010 Inspections of Domestic Annually Inspected Firms Regarding Deficiencies in Audits of Internal Control Over Financial Reporting
Observations from 2010 Inspections

- Identifying and testing of controls
- Obtaining sufficient evidence to update results of interim control testing
- Using the work of others
- Evaluating identified deficiencies and the effect on both the audit of internal controls and financial statement
- Documenting Management's review of controls
- Testing system generated data and reports
Observations from 2010 Inspections
Identifying and Testing Controls

Engagement teams failed to identify and sufficiently test controls that are intended to address the risk of material misstatement. The most common areas noted were:

1. Revenue
   – business units and categories
   - contract provisions
   - % completion inputs

2. Inventory – reserves and pricing of components
3. Fair value of financial instruments and disclosures
4. Valuation of pension plan assets.
Types of Testing, presented from least to most persuasive:

- inquiry
- observation
- inspection of relevant documentation
- re-performance

*Inquiry alone does not provide sufficient evidence to support a conclusion about the effectiveness of a control.*
Observations from 2010 Inspections
Rollforward Testing

Sufficiency of Rollforward Testing

• the specific control tested prior to year end, including the risks associated with the control and the nature of the control, and the results of those tests;

• the evidence of effectiveness of the operation of the control obtained at an interim date;

• the exposure period between interim and year end; and

• the possibility that there have been significant changes in internal control subsequent to the interim date.

*Inquiry alone is not a sufficient rollforward procedure for higher risk controls!*
Observations from 2010 Inspections
Using the work of others

Sufficiently perform procedures regarding the use of the work of others

- High risk areas
- Significant judgments
- Failed to re-perform
- Failed to validate key controls
Observations from 2010 Inspections
Evaluating deficiencies and their impact on audit

Sufficiently evaluate identified control deficiencies and consider their effect on both the financial statement audit and on the audit of internal control.

- evaluate whether AJEs / PAJEs are indicators of a control deficiency
- aggregation / other considerations in evaluating severity
- proper evaluation and testing of compensation control (precision)
Observations from 2010 Inspections
Management Review of Controls

Common examples of management review controls:

- Monthly comparisons of budget and actual results to forecasts for revenues and expenses
- Comparisons of other metrics, such as profit margins and certain expenses as a percentage of sales
- Quarterly balance sheet reviews
Observations from 2010 Inspections
Management Review of Controls

Testing involves performing procedures to obtain an understanding of and evaluating, on a test basis, the procedures performed in management's review

- Designed appropriately and operate at level of precision to detect material items
- How is management comfortable with completeness and accuracy of the data
- What is management criteria for investigation and is it appropriate
- Corroborating management's process
Use of IT effects the way transactions are initiated, recorded, processed and reported

Risk of improperly relying on applications that inaccurately process data or process inaccurate data

Need to test either controls over the system generated data and reports OR the completeness and accuracy of the data / reports
Observations from 2010 Inspections
Testing System Generated Data and Reports
(Completeness and Accuracy)

For example, some firms failed to:

• test IT general controls ("ITGCs") that are important to the
effective operation of the applications that generated the data or
reports,

• test the logic of the queries (or parameters) used to extract data
from the IT applications used in the reports, or

• address control deficiencies that were identified with respect to
the ITGCs over either the applications that process the data used
in the reports or the applications
that generated the reports.

APPLIES TO SUBSTANTIVE TESTING AS WELL
Observations from 2010 Inspections
Testing System Generated Data and Reports (Completeness and Accuracy)

When we talk about system-generated reports and data, what are we referring to?

Reports and other data coming from the IT systems used in:

• Tests of controls
  – Entity-level, including ITGC's
  – Activities-level
• Data used as inputs in computing estimates
Observations from 2010 Inspections
Testing System Generated Data and Reports (Completeness and Accuracy)

Identifying System-Generated Reports and Data – Watch list:

• Program change logs
• Security access reports
• Disaggregated data – revenue by month or product-line
• Ad hoc reports and queries
• Non-financial information – production data, sales data, etc.
• Reports and data provided to 3rd party service providers
Observations from 2010 Inspections
Testing System Generated Data and Reports (Completeness and Accuracy)

- Testing ITGC's alone is not sufficient
- ITGC's help ensure the continued, proper operation of information systems
  - Apply to all systems, not a specific process or report
- Just because ITGCs operate effectively, can't assume all information derived from the applications is complete and accurate
Observations from 2010 Inspections
Testing System Generated Data and Reports (Completeness and Accuracy)

Consider complexity of the report:

• How is it prepared: by who and what means
  – Separate report writing applications used?
  – Manual intervention?

• Source(s) of the information used to prepare the report
  – One or multiple systems/databases?
  – If multiple, integrated or operating on a stand-alone basis?
# Observations from 2010 Inspections

**Testing System Generated Data and Reports (Completeness and Accuracy)**

<table>
<thead>
<tr>
<th>Complex</th>
<th>Non-Complex</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Changes to existing applications, databases or systems</td>
<td>• Few changes to existing IT environment</td>
</tr>
<tr>
<td>• Creation of source code for in-house software</td>
<td>• Implementation of pre-packaged applications with no significant modifications</td>
</tr>
<tr>
<td>• Customized pre-packaged software adapted to client's needs</td>
<td>• User configurable options that don't significantly alter applications functioning</td>
</tr>
<tr>
<td>• Pre-packaged applications, changes and code put into production</td>
<td>• Lack of IT development projects</td>
</tr>
</tbody>
</table>
Observations from 2010 Inspections
Testing System Generated Data and Reports
(Completeness and Accuracy)

ITGC Process that Directly Affect Applications and Data

• Security administration: Enabling access to information to only those with legitimate business needs

• Batch program execution controls: Verifying only authorized application programs are executed against production data on a timely basis

• Change controls: Initiating change requests, designing, developing and configuring program changes and promoting changes to production
Observations from 2010 Inspections
Testing System Generated Data and Reports
(Completeness and Accuracy)

If a deficiency could impact the accuracy of the report, Companies need to:

• Obtain sufficient evidence that the deficiency didn't impact the report
• Document their conclusions
SOC Reports
Consideration of the scope & opinion

• Impact of a qualified SOC audit report on the Company's controls
  – Testing exceptions not addressed

• Report doesn't address the processes and controls that are important to the Company's control structure
  – Not considering processes that were carved out of the report
Consideration of user controls

- User controls noted in SOC audit report:
  - Not addressed/identified as an issue
  - Identified and evaluated, but not documented

- Must verify the implementation of user controls noted in the report in order to rely upon it
COSO Framework
Internal Control Over Financial Reporting: 
*Coso Framework*

- Updated internal control framework expected during Q1 2013
  - Clarifies certain terminology
  - Addresses the role of technology in internal control
  - Will not revise the definition of internal control or change its five essential components
- Original framework remains suitable and use will be accepted for a period of time
  - Registrants could implement the revised framework for December 2013 year-ends, if finalized in Q1 2013
- SEC may provide further transition guidance once the revised framework is finalized
Foreign Corrupt Practices Act
Why do we have the FCPA?
Globalization and competitive pressure

• Overseas expansion into developing countries
• Competitive pricing
• Unique risks and experience:
  – Economic espionage
  – Government corruption
  – Money Laundering
• Uneven regulatory playing field
FCPA
Provisions and Applicability

- **Anti-Bribery Provisions:**
  - Prohibits U.S. companies and citizens, foreign companies listed on a U.S. stock exchange, or any person acting while in the U.S. from paying or offering to pay, directly or indirectly, money or anything of value to a foreign official to obtain or retain business.
  - U.S. companies include its officers, directors, employees, agents, and stockholders

- **Books and Records and Internal Controls Provisions:**
  - Requires “issuers” (any company including foreign companies) with securities traded on a U.S. exchange or otherwise required to file periodic reports with the Securities and Exchange Commission (SEC) to keep books and records that accurately reflect business transactions and to maintain effective internal controls.
FCPA
Foreign Officials

• Any officer or employee of any department, agency, or instrumentality of a foreign government
• Foreign political party or official thereof
• Candidate for political office
• Any person acting in an official capacity for or on behalf of a foreign government, department, agency, or instrumentality
FCPA Influencing Official Acts

- Inducing foreign official to use influence with a foreign government or instrumentality thereof to affect any act or decision
  - Acts or decisions of foreign officials *in their official capacities*
  - Inducing foreign officials to do *or omit to do* any act in violation of lawful duty of such official
FCPA
Types of Illegal Payments

- Cash
- Checks and other financial instruments
- Gifts, travel and entertainment
- Hidden interest
- Loans
  - Alleged loan
  - Payments made or guaranteed
  - Interest free loan
- Credit card bills
- Transfers at less than fair market value
- Employment
- Concealing illegal payments
  - Off-book schemes
Facilitating payments

*Examples:*

- obtaining permits, licenses, or other official documents to qualify a person to do business in a foreign country
- processing government papers, i.e., visas, work orders
- providing police protection, mail pick-up/delivery, inspections
• Violation need not be fully consummated or succeed in desired outcome
• Applies to payments made by third parties when company knows that portion will be used for a proscribed purpose
FCPA
"Knowledge" Standards

• Does not require proof of actual knowledge
• Factual information indicating “high probability” of illegal activity
• Must follow up on “red flag” activity
FCPA Risk Factors

- Entity directly or through agents or representatives enters into sales agreements or material transactions with foreign governments, government-owned entities, or other officials
- Entity has operations in higher-risk geographies*
- Operations conducted in higher-risk industries (e.g., energy, defense, pharmaceuticals, medical devices, telecommunications) in higher-risk geographies
- The entity’s competitors, partners, suppliers, agents, or customers recently charged or being investigated for bribery or corruption violations
- Indications of possible bribery or corruption violations by employees, agents, contractors, or other affiliates
- Weak or ineffective anti-bribery and anti-corruption compliance programs
- The entity uses third-party agents, consultants, or intermediaries when performing business in other countries
FCPA
Risk Factors (con't)

- Decentralized management control
- Substantial payments to agents, consultants, or others for unspecified services
- Payments to offshore bank accounts, in cash or by wire transfer
- Unduly complex legal or banking structure
- Unusual payments for commissions, loans, legal fees, consulting, marketing, temporary employees and directors fees
- Payments and wire transfers without the proper approval process
- Payments to agents, etc. with unusual addresses
- Payments in round dollar amounts
- Unusually low or high profit margins on projects
- Undocumented business entertainment expenses
FCPA
Mergers & acquisitions

- DOJ Opinions and instances have established a pattern (not a binding position) for acquisition transactions.
- Acquiring company will not be held liable for pre-acquisition conduct provided it:
  - Promptly implements a compliance program
  - Discloses any pre-acquisition conduct it discovers
  - Cooperates in government’s investigation
- As economy rebounds M&A activity will resurge
- Successor liability is only diminished if FCPA due diligence is thoroughly conducted, identified issues rectified and compliance programs are implemented.
- Companies could lose their entire investment because they decided FCPA due diligence was not necessary.
FCPA Penalties

Companies
- Up to $2,000,000 or twice the gross gain/loss derived

Individuals
- Up to $250,000 or twice the gross gain/loss derived
- Up to 5 years imprisonment

**Accounting Provisions**

Companies
- Up to $2,500,000 fine

Individuals
- Up to $1,000,000 fine
- Up to 10 years imprisonment
FCPA
Anti-bribery and corruption compliance program elements

- Code of Conduct
- Tone at the Top
- Anti-Corruption Policies and Procedures
- Risk Assessment and Internal Control
- Annual Review
- Senior Management Oversight and Reporting
- Training and Annual Certifications

- Ongoing Advice and Guidance
- Discipline
- Confidential Reporting
- Agents and Other Business Partners
- Contractual Compliance Terms and Conditions
- Ongoing Assessment
- Acquisitions
- Investigative team that can be quickly mobilized
FCPA Components of Investigations

- Interview employees
- Computer forensics / e-discovery
- Public records search
- Select transactions for testing
  - Focus on certain accounts (marketing, training, legal, other receivables, payments to agents, anywhere payments could be “buried”) Review support for payments
- Compare data across sources – vendors and employees and any suspected names of government officials
- Review policy and procedure compared to practice
FCPA
How can payments for “unconsummated” actions be identified?

• Interviews
  – Sometimes you just need to ask.
  – Often employees do not hide facts (may not understand that it is an issue).

• Review detailed supporting documentation
  – Do the payments and patterns seem consistent with the business purpose?
  – Can the client explain what was accomplished by certain payments?
FCPA Investigation Challenges

- Language, culture
- Responsiveness may be less than with U.S. entities
- Data privacy issues
- Coordination of law firm, consultants and company
- Poor documents on which to base conclusions
  - e.g., participants not included in expense documentation
Final Questions?
This presentation is reprinted from Grant Thornton LLP’s “The Changing Regulatory Landscape" with permission. No portion of this presentation may be reprinted without express written permission from Grant Thornton LLP.

This presentation provides information and commentary on current accounting and tax issues and developments. It is not a comprehensive analysis of the subject matter covered and is not intended to provide accounting, tax, or other advice or guidance with respect to the matters addressed. All relevant facts and circumstances, including the pertinent authoritative literature, need to be considered to arrive at appropriate conclusions.

The information contained herein is general in nature and based on authorities that are subject to change. It is not intended to be, and should not be, construed as legal, accounting, or tax advice or guidance provided by Grant Thornton LLP to the reader. This material may not be applicable to or suitable for specific circumstances or needs and may require consideration of tax and nontax factors. Contact Grant Thornton LLP or another qualified professional adviser prior to taking any action based upon this information. Grant Thornton LLP assumes no obligation to inform the reader of any changes in tax laws or other factors that could affect information contained herein. No part of this document may be reproduced, retransmitted or otherwise redistributed in any form or by any electronic or mechanical means, including photocopying, facsimile transmission, recording, rekeying, or using any information storage and retrieval system, without express written permission from Grant Thornton LLP.