Welcome to 2017

For its April 8, 1966 issue, Time asked "Is God Dead" on its cover.

For its April 3, 2017 cover, the question "Is Truth Dead?"

Fraud Risk - Group Discussion

What are some examples of heightened fraud risk factors in most any industry?
Heightened Fraud risk factors:
- Inadequate internal controls over cash disbursements
- Financial Stress relating to employees or dissatisfaction with job-
  - Anticipated layoffs
  - No compensation adjustments
- Overbearing management –
- Change in lifestyle – complaining about finances
- Persons in key positions never take a vacation – Lack of job rotation

Recent findings from the Association of Certified Fraud Examiners (ACFE), 2006 Report to the Nations.
- Governmental fraud has the highest medium loss (100K State and 80K Local)
- A good percentage of frauds involve expense reimbursement

Victims of fraud:
- 82% had an external audit
- Over 80% had a code of conduct
- 60% had a confidential hotline
- 20% had required vacations and job rotations or employee rewards for whistleblowing

How were frauds detected:
- Lowest detective control - 4% of frauds detected by external audit
- Highest fraud detective control - Hotline
- Also rated high - Independent review of key transactions by management
Fraud In State and Local Governments

The top three contributors to fraud include
- Lack of documented internal controls
- Override of existing controls
- Lack of independent review

Who commits fraud
- Male –ages 31-45
- Educated
- Works in accounting department
- Worked in organization for several years

AICPA Standards

- AU-C section 315, Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement
- Identifies the same 5 interrelated components (as COSO and Green Book) that provide a useful framework for auditors when considering internal control
- Written from financial statement audit perspective

AICPA Standards

- On every audit the auditor must gain an understanding/update the client’s internal control before performing risk assessment
- This is probably the least understood requirement and results in audit deficiencies where there is inadequate linkage between documenting key internal controls, determining if they have been implemented, assessing risk of misstatement or fraud an completing further audit procedures –

Key point
- Conducting Risk Assessment procedures
COSO/ Green Book – 3 Objectives of Internal Control

1. Efficiency and effectiveness of operations-(Safeguarding of assets)
2. Sound Financial Reporting
3. Compliance with Laws and regulations

Key Point
Auditors are primarily focused on financial reporting and only those objectives relevant to the audit if they have effect on FS or disclosures.

Group Exercise

› What are some common sense questions you should ask as you begin to gain an understanding of the client’s system of internal control?

Internal Control Requirements

› Example of common sense questions:
1. What external risks -economic, industry or your own business risks did your company face this past year?
2. How do you measure your financial performance throughout the year?
3. What are 2-3 preventative/detective fraud controls you rely on month to month throughout the year?
4. If an error were to occur in the financial statements how is it going to be detected?
5. If a key person were to leave unexpectedly in your accounting department, how do you ensure there wouldn’t be material errors occurring?
Internal Control Requirements

› Ask common sense questions regarding specific applicable compliance requirements
  1. What are the resources you use to understand the requirements and manage your indirect cost rate?
  2. How do you ensure only allowable costs are charged?
  3. If an error were to occur how is it going to be detected?


› Consists of three volumes:
  - Executive Summary Framework and Appendices
  - Illustrative Tools for Assessing Effectiveness of a System of Internal Control

› Sets out:
  - Definition of internal control
  - Categories of objectives
  - Components of internal control
  - Requirements for effectiveness

The Green Book

› Updated in September 2014
› Written primarily for federal government
  - Leverages the COSO Framework
  - Uses government terms
› The Green Book states that it may also be adopted by state, local, and quasi-governmental entities, as well as not-for-profit organizations, as a framework for an internal control system
The non-federal entity must establish and maintain effective internal control over the federal award that provides reasonable assurance that the non-federal entity is managing the federal award in compliance with federal statutes, regulations, and the terms and conditions of the federal award.

Internal controls should be in compliance with guidance in:
- "Standards for Internal Control in the Federal Government" (Green Book) issued by the Comptroller General of the United States, and
- the "Internal Control Integrated Framework", issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Key Point
Use of "should" in Uniform Guidance indicates a "best practice" and is not a presumptively mandatory requirement

COSO/Green Book

Key Point
- A deficiency exists in an entity system of internal control when a component and one or more of its principles are not present or functioning

COSO/Green Book

Key Point
- The Green Book states that an entity should document when a principle is deemed unnecessary and how the entity was able to meet the related objective(s)
**COSO/Green Book – 5 Components of Internal Control**

1. Control Environment
2. **Risk Assessment**
   - Least understood by auditors
3. Control Activities
4. Information and Communication
5. Monitoring

**COSO/Green Book**

Revised COSO Framework

**Major changes**
- 17 principles allocated across the 5 components to assist in understanding the requirements for effective internal control.

**Key Points:**
- Auditing standards do not set up a lower standard for smaller entities or for different industries
- Principles generally align with AU-C section 315

**COSO/Green Book**

Five related principles

- **Control environment**
  1. Commitment to integrity
  2. Independence of board
  3. Structure, reporting lines of authority, responsibility assigned
  4. Commitment to competency
  5. Accountability across IC responsibilities
**COSO / Green Book**

**Commitment to integrity**
- Sets tone at the top
- Established code of conduct
- Whistleblower policy
- Regular staff meetings
- Ethics hotline
- Upward evaluations

**COSO / Green Book**

**Commitment to Structure, reporting lines of authority and accountability, competency**
- Written accounting and financial policies
- Recruitment
- Evaluations – Competency
- Succession of leadership
- Accountability
- Mitigate excessive pressure on expectations
  - Concern employees will cut corners

**COSO / Green Book**

**Four related principles**

**Risk Assessment**
1. Establishes clear objectives
2. Identify and assess internal & external control risks
3. Identifies fraud risks
4. Identifies and analyzes significant changes that could impact internal control
COSO / Green Book
Risk Assessment
- Identify Risks that prevent the entity from achieving objectives
- Analysis of risk – Magnitude, likelihood and nature
- Respond to risks (Accept it, reduce it or avoid it)

COSO / Green Book
Risk Assessment
Internal Risks
- Complex accounting transactions or complex systems and programs - Material grants
- High public interest and reaction to fraud, waste and abuse
- Organizational – Relationship with component units

COSO / Green Book
Risk Assessment
External Risks
- Changes to laws and regulations
- Changes to accounting and financial reporting principles
**Risk Assessment**

**Fraud Risks**
- Laws and regulations governing general operations and its component units
- Theft of assets
- Management overriding its own controls

---

**Fraud Risks**
- Preventive controls
  - Separation of duties-independent check on performance
  - Reconciliations
- Detective controls
  - Fraud hotline

---

**Three related principles**

- **Control Activities**
  1. Aligns controls to mitigate risks
  2. Selects and develops IT general controls
  3. Establishes internal control policies and procedures and **implements them**
COSO / Green Book

Control Procedures
- **Proper authorization** - Specific and general
- **Separation of duties** - independent check on performance
- **Reconciliations**
- **Proper written policies** - including number and nature of funds – when established – or eliminated
  - General controls over IT environment – Passwords, cyber security
  - Application (input, processing and output controls)

COSO / Green Book

Three related principles
- **Information and Communication**
  1. Information is relevant to the IC objectives
  2. Internally communicates information to support IC
  3. Externally communicates IC matters

COSO / Green Book

Two principles
- **Monitoring**
  1. Selects develops and performs ongoing monitoring – How budget is balanced in economic stress periods
  2. Internally communicates deficiencies to responsible parties for corrective action
Exercise – Identify each control as entity or activity level?

<table>
<thead>
<tr>
<th>Entity level</th>
<th>Activity level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control environment</td>
<td>✓</td>
</tr>
<tr>
<td>Risk assessment</td>
<td>✓</td>
</tr>
<tr>
<td>Control activities</td>
<td>✓</td>
</tr>
<tr>
<td>Information and communication</td>
<td>✓</td>
</tr>
<tr>
<td>Monitoring</td>
<td>✓</td>
</tr>
</tbody>
</table>

COSO Internal Control Elements

<table>
<thead>
<tr>
<th>Entity level</th>
<th>Activity level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control environment</td>
<td>✓</td>
</tr>
<tr>
<td>Risk assessment</td>
<td>✓</td>
</tr>
<tr>
<td>Control activities</td>
<td>✓</td>
</tr>
<tr>
<td>Information and communication</td>
<td>✓</td>
</tr>
<tr>
<td>Monitoring</td>
<td>✓</td>
</tr>
</tbody>
</table>

Entity Level Controls vs. Activity Level

US GAAS requires:
- Assess the risk of material misstatement at both financial statement level and transaction/cycle level and assertion level
Entity Level Controls vs. Activity Level

Entity level controls are pervasive, therefore focus on entity wide controls first -

Key Point
This is a real problem with real life risk assessment, as we will discuss later.

To Summarize:
- Entity level controls are pervasive, therefore our response is on the overall engagement such as:
  - Engagement team staffing
  - Timing of audit procedures
  - Review and Supervision
  - Plan for higher inherent risk assessments at the activity level.

Your consideration of entity level controls should be in the context of achieving principles or control objectives relevant to the preparation of financial statements that are free of material misstatement.

Key Point
- You need to document whether the client's system of internal control addresses each principle and the one or more key control(s) were implemented during the year evidencing the principle -
COSO – 5 Components of Internal Control

Let’s review some examples:
1. Control Environment
2. Risk Assessment
3. Control Activities
4. Information and Communication
5. Monitoring

Control Environment

**Principle:** The entity demonstrates a commitment to integrity and ethical values. Control – A code of conduct or ethical policy exists at (WP reference).

**Principle:** The governing body demonstrates independence from management in exercising oversight of the development and performance of internal control over financial reporting. Control – the makeup and general construction of the board is appropriate given the nature of the entity. See the makeup of the board and various committees at (WP reference).

Control Environment

**Principle:** The entity demonstrates a commitment to develop and retain competent individuals in alignment with financial reporting objectives. Control – Management conducts periodic evaluations of its personnel and offers outside training opportunities. See evaluation form for name and name’s attendance at an accounting seminar. See WP section.
COSO – 5 Components of Internal Control

Risk Assessment

Principle: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to internal risks associated with key personnel changes, communication of key IT general controls & application controls and has an accounts payable accounting policy manual to ensure vendor set up and monitoring occurs.


Principle: The entity considers the potential of fraud in assessing risks to the achievement of financial reporting objectives.

Control: Those charged with governance understand and exercise oversight by managing the entities fraud hotline and review of upward evaluations.

COSO – 5 Components of Internal Control

Information and Communication

Principle: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control over financial reporting.

Control: Financial personnel meet with management to discuss operating results. (Name) is the organization’s Business Manager and also is responsible for compiling the financial statements. (Name) creates financial statement narratives to describe significant changes from the prior year or budget and presents to the board. See copy of May board summary at (WP section).

COSO – 5 Components of Internal Control

Information and Communication

Principle: The entity externally communicates information, necessary to support the functioning of internal control over financial reporting.

Control: In house financial statements are prepared quarterly. The financial statements are reviewed by the governance. See copy of May board summary at (WP section). Inquired with (name) and the statements were submitted quarterly during the year.
COSO – 5 Components of Internal Control

Monitoring

Principle: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action.

Control – Deficiencies in internal control are reported to management and governance on a timely basis. Operational issues are reported by the operations manager to governance. All accounting issues or control deficiencies are communicated to the Finance committee during the audit process. We have noted no repeat findings, and scanned prior year communications to governance regarding repeat findings.

True or False

Question

- If you assess control risk, you must test the operating effectiveness of control in the current year. Your assessment of control risk below maximum in connection with the transaction class or account, based on controls tested in a prior year is not appropriate.

Answer – True

- If you assess control risk, you must test the operating effectiveness of control in the current year. Your assessment of control risk below maximum in connection with the transaction class or account, based on controls tested in a prior year is not appropriate.

Source: AU-C-section 330 Par.15
Example Accounts Payable Cycle

Control Procedures over accounts payable accounts Internal and external Risks

- Lack of separation of duties within AP-No review of account coding: Significant Risk & Fraud Risk
- No pre-approval of vendor set up into the AP system
- No monthly reconciliation of AP and accruals documented
- A large number of transaction flow through AP monthly
- Key high risk accounts are listed and maintained by AP clerk, as found in AASHTO Guide Section 10

Risk Assessment – AP Cycle

<table>
<thead>
<tr>
<th>Account</th>
<th>S-Significant F/Fraud Risk</th>
<th>Inherent Risk</th>
<th>Control Risk</th>
<th>Risk of Material Misstatement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounts Payable – cash expenditures Relevant Assertions:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Occurrence</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• GL Coding/Classification</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Cut-off</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(F)Lack of duties</td>
<td>H</td>
<td>L</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>(F)Fraud – Code unallowable as allowable</td>
<td>H</td>
<td>H</td>
<td>L</td>
<td>L</td>
</tr>
</tbody>
</table>

Example- Payroll Cycle

Control Procedures over Payroll Internal and external Risks

- Timesheet for non-exempt employees not always maintained to document time spent on marketing and business development
- All timesheets are reviewed for direct and overhead payroll and related payroll items like overtime, paid time off and holiday
- Authorized pay rates, adjusted annually are maintained in personnel file
Account | S-Significant F-Fraud Risk | Inherent Risk | Control Risk | Risk of Material Misstatement
--- | --- | --- | --- | ---
Payroll Relevant Assertions: Occurrence Accuracy Classification | Fraud risk: Unallowable labor charged to allowable code | L | L | L

Entity level controls, not pervasive can provide cost effective ways to limit your response to unusual or new accounting transactions.

**Example**
- The client’s system has been historically effective for routine transactions but not for new accounting standards or regulations.

**Key Point**
- Risk is only linked to new regulations.

**Risk Assessment**

Paragraph .04 of AU-C Section 315 defines a significant risk as a risk of material misstatement that in your judgment requires special audit consideration.

**Key Point**
- One or more significant risks arise on most audits.
Risk Assessment
Special audit consideration means respond as follows:

1. Obtain understanding of control relevant to that risk and determine if implemented
2. Perform an audit procedure linked clearly to that risk
   Must be more than analytical review

Example Controls: “Allowable and Unallowable costs”

- **Control Environment**
  - Management sets reasonable indirect cost budgets - minimize incentives to miscode expenditures
  - Management provides training under applicable part 31.2 of FAR

- **Risk Assessment**
  - Management has sufficient understanding of procedures and controls to identify unallowable costs and requests periodic update by program managers on program compliance

- **Information and Communication Systems**
  - Comparison of budget to actual rates is provided to project manager for review on a timely basis

- **Control Activities**
  - Program managers approve purchase orders/invoices prior to payment

- **Monitoring**
  - Financial reports provided to appropriate management on periodic basis for review

THANK YOU!