The “How To” on Fraud Risk Assessment

Monica Frazer, CPA
Vice President, Internal Audit
Baylor Health Care System
Agenda

- Expectations for Fraud Risk Assessments
- Antifraud Programs and Controls
- Methodology
- Importance of Communication
- Benefits of a Fraud Risk Assessment
An entity-wide examination of a company’s vulnerability to potential fraud schemes.
Companies are expected to perform fraud risk assessments.
- Increased legislation, regulatory requirements, and professional guidance.
- Renewed focus due to high-profile scandals.
- Good business practice.
302 (Quarterly Certifications)
Management discloses to the independent auditors and Audit Committee any fraud that involves management or other employees having a significant role in the company’s internal controls.

404 (Annual Assertion)
Management’s assertion regarding effectiveness of internal controls over financial reporting (ICFR) – defined by SEC to include controls related to “prevention, detection and identification of fraud.”
The Sarbanes-Oxley Act requires that each company have a documented and on-going process to identify, assess, and evaluate fraud risks related to internal control over financial reporting.
- Emphasizes importance of antifraud controls.

- Requires independent auditors to evaluate the fraud-related activities of the internal audit department annually.
8B2.1 (Effective Compliance and Ethics Program): Accepted universally as the benchmark of an effective program.

DOJ and SEC use for charging and sanctioning decisions.

Requires periodically assessing the risk that unlawful conduct will occur.

2004 amendments create substantial overlap between USSG and Sarbanes-Oxley requirements for antifraud programs.
Explicitly requires management to conduct a fraud risk assessment of corruption, fraudulent financial reporting, and asset misappropriation.
1210.A2 – Internal auditors must have sufficient knowledge to **evaluate** the **risk** of **fraud** and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.
- Perform or evaluate management’s fraud risk assessment.

- Consider fraud risk in developing the annual audit plan.

- Be alert to circumstances giving rise to fraud.
- Assist management pursue discipline and prevent occurrence.

- Help design external and internal communication.

- Form an opinion on internal control related to fraud.
IIA Standard 1220: Due Professional Care

1220.A1 – Internal auditors must exercise due professional care by considering the...Probability of significant errors, fraud, or noncompliance.
Reporting must also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the board.
2120.A2 – The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.
IIA Standard 2210: Engagement Objectives

2210.A2 – Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.
Fraud risk assessments should be an integral component of an organization’s antifraud programs and controls.
Essential Elements

- Tone at the Top
- Code of Conduct
- Monitoring Activities
- Whistleblower Hotline
- Fraud Risk Assessment
- Fraud Training & Awareness
- Hiring & Promotion Procedures
A fraud risk assessment is the cornerstone of an antifraud program that anticipates, rather than reacts to, fraud and misconduct.
Develop a methodology.
- Establish a framework
- Identify fraud risks
- Assess fraud risks
- Evaluate existing controls
- Develop a remediation plan
- Integrate with annual audit plan
As the central guide for the assessment process, the framework provides a structure for assessing the fraud risks and related controls.

- Fraud Risk Matrix (Excel spreadsheet)
- Primary document for collecting assessment data
- Captures:
  - identified fraud risks
  - assessment of risks
  - mitigating controls
  - remediation plans
<table>
<thead>
<tr>
<th>Fraud Scenario</th>
<th>L</th>
<th>I</th>
<th>Results (LxI)</th>
<th>Antifraud Controls</th>
<th>Evaluation of Antifraud</th>
<th>Control Gaps</th>
<th>Remediation Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company would conduct business with a vendor owned by an employee/friend or family member of an employee</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Company would make illegal copies of software or install software beyond what is allowed by licensing agreement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee would assist vendor in winning a bid for a project</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee would install software with the purposes of controlling, damaging or stealing data to allow unauthorized access to the network</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employees would steal patient information for the purposes of identity theft</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physician would not be paid in accordance with an executed contract</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fraud Scenario</td>
<td>L</td>
<td>I</td>
<td>Results (LxI)</td>
<td>Antifraud Controls</td>
<td>Evaluation of Antifraud</td>
<td>Control Gaps</td>
<td>Remediation Steps</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------</td>
<td>---</td>
<td>---</td>
<td>---------------</td>
<td>--------------------</td>
<td>------------------------</td>
<td>--------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Patients would be charged for services not provided</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physician is occupying space without paying rent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee would up-code in order to increase revenue</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee would intentionally manipulate the books and records to meet budget or expectations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Through management interviews, historical trend analysis, and external research, a fraud risk universe is developed.

- Includes all possible fraud schemes that could impact your company

- Schemes are classified according to the Uniform Occupational Fraud Classification System (Association of Certified Fraud Examiners)

- Interviews with management provide experienced insight into actual and potential fraud schemes
An assessment is conducted for each risk scheme to ensure an appropriate response.

- Each risk is evaluated in terms of likelihood and impact
- Likelihood assessment assigns a numeric ranking to the *inherent* probability that the risk will occur, *assuming no controls* in place to mitigate the risk
- Impact assessment assigns a numeric ranking to the impact the risk would have on the organization if it occurred:
  - Financial loss or misstatements within the financial statements.
  - Consequences of fraud on the company’s reputation.
  - Impact on operations
- Risks assigned to Fraud Risk Map
To prioritize mitigation efforts and effectively allocate resources, each risk is assigned to a quadrant on the Fraud Risk Map. The purpose of the Fraud Risk Map is to guide the appropriate response for each potential fraud scheme.
For each fraud risk, mitigating controls are identified and evaluated.

Controls are evaluated based on two criteria:

**adequacy of design**

Considers whether, if the identified controls operate as designed, the fraud risk will be adequately mitigated.

**effectiveness of operation**

Considers whether a properly designed control is operating as designed and whether the person performing the control has the necessary authority, skill, and qualifications to perform the control effectively. Evaluating operating effectiveness involves testing the controls.
Plans are developed to remediate any residual fraud risks.

- Residual risk = risk not adequately mitigated by antifraud programs and controls

- Process owners are required to develop a remediation plan

- Internal Audit will follow up and report on management’s progress toward implementing the plan
Risks identified through the fraud risk assessment are factored into annual audit planning.

- Results are integrated with the annual risk assessment
- Annual risk assessment is performed to ensure that significant financial, operational, and information systems risks are appropriately addressed
- Audits are prioritized based on their relative level of risk, which includes multiple risk factors in addition to fraud risk
Communication is paramount for a successful fraud risk assessment.
The message:

- What is the definition of fraud?
- Why perform a fraud risk assessment?
- How will the information be used?
- Who will have access to the information?
- How does a fraud risk assessment differ from the annual risk assessment?
- What level of resources will be required?
The approach:

- Start at the Top
- Communicate at All Levels
- Communicate Inside & Outside the Audit Department
- Communicate Often
- Listen Well
The benefits of a fraud risk assessment are numerous.
For the company:

- Safeguard brand value and reputation
- Increase earnings
- Meet IIA, SEC, SOX, and other standards and requirements for antifraud programs and controls
- Mitigate SEC and Department of Justice sanctions
For Internal Audit:

- Another Value-Added Activity
- Leading Role in a High-Visibility Area
- Complements the Annual Risk Assessment
- Excellent Training for Staff
- Platform for Partnerships
Yes, it really is that important...
The Take-Away

Facilitating a comprehensive fraud and reputation risk assessment is the single-most important contribution that Internal Audit can contribute to an organization’s antifraud programs and controls.

PricewaterhouseCoopers
The Emerging Role of Internal Audit in Mitigating Fraud and Reputation Risks
Thank You!

Monica Frazer

monica.frazer@baylorhealth.edu

214.820.8327
Save the Date: August 26-29, 2012

31st Annual Conference in Philadelphia, Pennsylvania

ahia
Assoc. of Healthcare Internal Auditors