A Moment of Truth about Potential Fraud in your Organization: Performing Fraud Risk Assessments

Presented by:
Christy Decker, John Lefter & Michael Mena
Sharp HealthCare
Wednesday, September 10, 2014
Christy Decker is the Vice President of Internal Audit Services at Sharp HealthCare in San Diego, CA. Since joining Sharp HealthCare in 2005, Ms. Decker has been responsible for performing and managing operational, financial and compliance audits. Ms. Decker is a Certified Public Accountant (CPA), Certified Internal Auditor (CIA), Certified in Risk Management Assurance (CRMA) and Certified Fraud Examiner (CFE). She has a BS from San Diego State University in Accounting and Spanish. Past positions include three (3) years public accounting experience with KPMG and three (3) years of other auditing and accounting experience. She is currently the West Region District Advisor for the Institute of Internal Auditors (IIA).

John Lefter is the Manager of Internal Audit Services at Sharp HealthCare. Since joining Sharp in 2012, John has been responsible for managing operational, financial and compliance audits together with Christy. John is Certified in Risk Management Assurance (CRMA) and a Certified Information Systems Auditor (CISA). He has a BS in Finance from San Diego State University and an MS in Accounting from University of Notre Dame. Past positions include five (5) years public accounting experience with EY and five (5) years of internal audit experience in the defense and healthcare industries. He is currently the President of the San Diego Chapter of the IIA.

Michael Mena a Senior Internal Auditor at Sharp HealthCare. Since joining Sharp in 2012, Michael has been responsible for performing operational, financial and compliance audits. Michael is Certified in Risk Management Assurance (CRMA), Certified Internal Auditor (CIA), Controlled Self Assessments (CCSA) and Certified Fraud Examiner (CFE). He has a MBA from Cal State San Bernardino. Past positions include six (6) internal audit experience in government and three (3) accounting experience in the private sector. He is currently a Webmaster for the San Diego Chapter of the IIA.
Today’s Outline

• Overview of Sharp HealthCare and the Internal Audit Services Department

• Fraud Risk Defined

• Why Perform a Fraud Risk Assessment?

• Seven Elements of an effective anti-fraud program

• Sharp HealthCare’s approach to completing a Fraud Risk Assessment

• Reporting the results to Management and the Audit Committee
San Diego’s Health Care Leader℠

- Not-for-profit serving 3 million residents of San Diego County
- Sharp has grown from one hospital in 1955 to an integrated health care delivery system
- Largest health care system in San Diego with highest market share
  - 4 acute care hospitals, 3 specialty hospitals, 2 affiliated medical groups and a health plan, plus a full spectrum of other facilities and services with the most complete range of health care services in San Diego
  - Market share leader and only health system that increased market share each of the past 12 years
- Largest private employer in San Diego
  - 16,400 employees, 2,600 physicians and 2,800 volunteers
Sharp HealthCare Internal Audit Services

- Reports to CEO and Board Audit and Compliance Committee

- Oriented to adding value through identification of improved controls, revenue enhancements and cost savings and recoveries

- Contributes to improving overall control environment through innovative services

- Seven and ¾ Professional Full-time Equivalents (FTEs)

- Staffing Characteristics:
  - Aptitude for creativity, initiative, service and general business sense
  - Technical competency and professional certification
Definition of Fraud

Any intentional act committed to secure an unfair or unlawful gain.
Profile of a Fraudster

- Feels undercompensated or under appreciated
- Under pressure due to excessive lifestyle
- Want to achieve their ambitious financial goals
- Has worked in company more than 10 years, is considered a trusted employee and is in a position of responsibility
- Takes advantage of:
  - Weak internal controls
  - Excessive trust placed in him/her
  - Sufficient freedom
"Red Flags" In Employee Behavior

- Living beyond means
- Financial difficulties
- Control issues, unwillingness to share duties
- Unusually close association with vendor/customer
- Wheeler-dealer attitude
- Divorce/family problems
- Irritability, suspiciousness or defensiveness
- Addiction problems
- Unusual generosity
- Missing or incomplete documents

- Refusal to take vacations
- Past employment-related problems
- Complains about inadequate pay
- Excessive pressure from within organization
- Past legal problems
- Instability in life circumstances
- Excessive family/peer pressure for success
- Complains about lack of authority
- Conspicuous change in behavior (dominating, absolute behavior)
Why Perform a Fraud Risk Assessment?

Why is a fraud risk assessment important?

- U.S. organizations lose approximately 5% of their annual revenues to fraud (2014 ACFE Report to the Nations). Applied to the 2013 Gross World Product, this figure translates to a potential projected annual fraud loss of more than $3.7 trillion. The median loss caused by the occupational fraud cases in the study was $145,000. More than one-fifth of these cases caused losses of at least $1 million.

- With an established and effective fraud program and periodic assessment of fraud risks, all employees should be empowered to identify organizational vulnerabilities and be able to play a role with the following:
  - Minimizing revenue leakage, cutting costs, and safeguarding assets.
  - Safeguarding company and employee reputation, and employee morale.
  - Avoiding and/or reducing criminal, civil and regulatory penalties, should misconduct occur.
  - Help avoid/reduce government sanctions.
  - **Take fewer antacids and sleep a little better at night!**
Why Perform a Fraud Risk Assessment?

The IIA Standards and Fraud

- **International Standards for the Professional Practice of Internal Auditing (Standards)**
  - Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization.
  - The chief audit executive must report periodically to senior management and the board [...] significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the board.
  - The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.

- **Per The IIA, The American Institute of Certified Public Accountants (“AICPA”) and Association of Certified Fraud Examiners (“ACFE”) in their “Managing the Business Risk of Fraud: A Practical Guide”**
  - Organization stakeholders have clearly raised expectations for ethical organizational behavior. Meanwhile, regulators worldwide have increased criminal penalties that can be levied against organizations and individuals who participate in committing fraud.
  - Organizations should respond to such expectations. Effective governance processes are the foundation of fraud risk management.
Why Perform a Fraud Risk Assessment?

2013 COSO Framework

Principle 8: The organization considers the potential for fraud in assessing risks to the achievement of objectives.
- Considers various types of fraud
- Assesses incentives and pressures
- Assesses opportunities
- Assesses attitudes and rationalizations
When Fraud Happens

The impact of misconduct and dishonesty may include:

- Actual financial loss
- Damaged reputation of the organization and employees
- Cost of investigation
- Loss of employee
- Loss of customers/patients
- Damaged relationships with vendors and suppliers
- Litigation
- Damaged employee morale
Seven Elements of an Effective Anti-Fraud Program

Set the Tone
- A. Code of Ethics
- B. Fraud Prevention Policies
- C. Communications and Training

Proactive Elements
- D. Fraud Risk Assessment
- E. Controls Monitoring

Reactive Element
- F. Fraud Response Plan

Overall
- G. Ownership of the Anti-fraud Program

Sharp HealthCare’s approach to completing a System-wide Fraud Risk Assessment

Example Agenda for the Angels & Demons Sessions

<table>
<thead>
<tr>
<th>Steps</th>
<th>Minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reflection &amp; Introductions</td>
<td>5</td>
</tr>
<tr>
<td>Ice Breaker</td>
<td>10</td>
</tr>
<tr>
<td>Sample Fraud Scenarios</td>
<td>10</td>
</tr>
<tr>
<td>Demon Brainstorming</td>
<td>30</td>
</tr>
<tr>
<td>Report Out &amp; Discussion</td>
<td>25</td>
</tr>
<tr>
<td>Break</td>
<td>10</td>
</tr>
<tr>
<td>Angel Brainstorming</td>
<td>30</td>
</tr>
<tr>
<td>Report Out &amp; Discussion</td>
<td>25</td>
</tr>
<tr>
<td>Break</td>
<td>10</td>
</tr>
<tr>
<td>Prioritization and Ranking with Scorecards</td>
<td>10</td>
</tr>
<tr>
<td>Identify Action Items</td>
<td>10</td>
</tr>
<tr>
<td>Wrap-up</td>
<td>10</td>
</tr>
<tr>
<td>• Survey</td>
<td></td>
</tr>
<tr>
<td>• Questionnaire</td>
<td></td>
</tr>
</tbody>
</table>
Reflection and Ice Breaker

Reflection: “Fraud and falsehood only dread examination. Truth invites it.” – Samuel Johnson, English Poet

Ice Breaker:
• Name

• Company, Title

• Finish the statement, “If you had to choose your last meal, what would it be?”
Sample Fraud Scenarios

Five Indicted At Johns Hopkins Hospital For Identity Theft Scam - Insiders allegedly used patient records to obtain more than $600,000 worth of credit

- A federal grand jury has indicted Jasmine Amber Smith, age 25, of Nottingham and four others on fraud and aggravated identity theft charges in connection with a scheme to use stolen hospital patient identity information to open fraudulent credit accounts and make purchases on “instant credit” at retail stores in Maryland.

- According to the 39 count superseding indictment, while employed by Johns Hopkins Hospital from August 2007 to March 2009, Smith is alleged to have improperly accessed the records of the hospital’s patients to obtain the personal identity information of patients and the parents and guardians of minor patients, including names, social security numbers, dates of birth and addresses. Smith allegedly provided the stolen identity information to apply for instant credit at stores located in Maryland and make purchases on “instant credit” before the fraudulently-obtained credit cards were received by the victims.

- The indictment alleges that during the course of the scheme, the defendants fraudulently obtained over $600,000 in credit from over 50 institutional and individual victims.

- The defendants face a maximum sentence of 30 years in prison.

Source: U.S. Attorney’s Office, District of Maryland or http://www.phiprivacy.net/?p=4042
Demon Brainstorming

- For each session, we had the group split into two groups
- Within each group, the groups brainstormed potential fraud schemes that could occur within the processes/business unit(s) they work in and/or manage.
- Using flip charts, notated the potential fraud schemes identified and the following:
  - Who is the perpetrator?
  - How did it occur? How can it happen?
  - What are the incentives or pressures, if any?
  - How could it be covered up?
- Think Like A Criminal!
  - What could happen if a criminal were a vendor or customer?
  - How could a criminal manage to do within your business unit?
  - What if a trusted employee begins to think or act like a criminal?
  - What if a criminal were hired as an associate?
- Subsequent report out and discussion
  - Selected a representative from each group to present the potential fraud schemes identified
  - Group discussion, comments and questions
Angel Brainstorming

• Each group switched to the other set of scenarios
• Within each group, reviewed the potential fraud schemes identified on the flip charts and notated the following:
  – What processes and controls are in place to prevent this?
  – What processes and controls are in place to detect this?
  – What gaps or opportunities still exist?
  – Potential solutions or recommendations?
• Subsequent report out and discussion
  – Selected a representative from each group to present the potential fraud schemes identified
  – Group discussion, comments and questions
Prioritization and Ranking with Scorecards

- Each participant completed the scorecard provided to risk rank each potential fraud scheme identified in their session.

- For each fraud scheme notated, rank the likelihood and impact for each, as follows:
  - **Likelihood:** Consider if the fraud has occurred in the past and other factors, such as, complexity, number of transactions, number of people reviewing and approving the process.
  - **Ranking:** Remote (1); Reasonably possible (3); or Probable (5)

  - **Impact:** Consider not only the monetary significance but also the implication to Sharp’s operations, brand value, reputation, and criminal, civil and regulatory liability.
  - **Ranking:** Inconsequential (1); More than inconsequential (3); or Material (5)
Session Wrap-up

• Discussed and shared as a group any items immediately actionable
• Final comments

Summary – Conducted 8 workshops of three hours each, with 110 employee participants
Session Follow-up

For each session held:

• Post-meeting survey and anti-fraud questionnaire sent to all participants

• All identified scenarios were computed with the average rating from the individual scorecard results and were shared with participants, along with any action items identified during the session
Final Steps

For all sessions held:

• Scorecard results were combined for all sessions
• Ranked from highest to lowest (on a rating scale of 1-5)
• Selected a median score and analyzed the results of those greater than the median
• These scenarios fell into six basic categories
Final Steps (continued)

- Shared the top five categories, including more detailed sub-categories to the “Fraud Steering committee” (HR, Legal, Compliance, Finance, IT, Security)
- Action plans were developed and documented for each sub-category and followed-up on quarterly
Reporting to the Audit Committee

A summarized report of the overall anti-fraud program assessment, including the summarized results of the Angels & Demons sessions, was presented to the Audit and Compliance Committee.
Reference Material

- IIA IPPF 2013
- “Managing the Business Risk of Fraud: A Practical Guide”, Non-binding guidance, jointly sponsored by IIA, AICPA & ACFE
- IIA Knowledge Alert: “Emerging Trends in Fraud Risks”, January 2010
- “ACFE Fraud Prevention Check-Up”, ACFE
- COSO 2013 Internal Control - Integrated Framework
Contact Information

Christy Decker
VP Internal Audit Services
Sharp HealthCare
Phone: 858-499-5508
Email: christy.decker@sharp.com

John Lefter
Internal Audit Services Manager
Sharp HealthCare
Phone: 858-499-3531
Email: john.lefter@sharp.com

Michael Mena
Senior Internal Auditor
Sharp Healthcare
Phone: (858) 499-3107
Email: michael.mena@sharp.com
Thank you!

Questions?
Comments?
CPE Code:

SK3W984