Fraud Risk Assessments: The Foundation of an Anti-Fraud Program

W. Noel Haskins–Hafer
CFE, CRMA, CISA, CISM, CGEIT, CRISC, SCPM
13 February 2013

Agenda

- Fraud Risk Assessment Definition
- Characteristics of Effective Fraud Risk Assessments
- Fraud Risk Assessment Planning
- Fraud Risk Assessment Framework
- Fraud Risk Assessment Tips
What is Fraud?

- A knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment

*Black’s Law Dictionary*

Fraud Risk Assessment Defined

- An assessment of the potential for fraud to affect an organization’s ability to maintain operations and reputation
- Identifies and addresses an organization’s vulnerability to both internal and external fraud

*Charles Ponzi*
Why Assess Fraud Risk?

- Understand where fraud could occur
- What affect fraud could have on the organization
- Allow informed decisions on what, how, and if to address

Identify and prioritize the risk of fraud

Benefits of an FRA

- Improve communication and awareness of fraud
- Know who and what puts the organization at the greatest risk
- Drive preventive actions
- Develop methodology for detecting, validating and investigating fraud
- Assess internal fraud controls
- Comply with regulations and standards
An Effective FRA…

- Suits the organization’s culture
- Encourages open and ongoing participation
- Has independent and authoritative sponsorship
- Is collaborative
  - Management and auditors especially
- Is independent and objective
- Requires working knowledge of the business

An Effective FRA also…

- Accesses all levels of the organization
- Engenders trust through leadership
- Thinks the unthinkable
- Considers value and risk of fraudulent activities
- Evolves with the business
**Getting Started**

- Assemble the right team
- Identify data gathering and analysis techniques
- Get sponsorship and agreement
- Educate the employees
- Promote the process

*Make people feel comfortable about participating*

---

**FRA Strategic Thinking**

- How could a fraud exploit weaknesses in controls
- How could controls be overridden or circumvented
- How could fraud be concealed

---

Martin Frankel’s To-Do List
*Item 1: Launder money*
FRA Framework

- Identify potential fraud risks
  - Incentives, pressures and opportunities
  - Management overrides
  - External factors
  - Regulatory or legal misconduct
  - Reputation
  - Information technology

FRA Framework, continued

- Assess likelihood of occurrence
- Assess fraud risk significance and impact
- Identify fraud-prone positions and departments
- Understand potential fraud scenarios
- Identify and map preventive and detective controls to fraud risks
- Evaluate effectiveness of controls
- Determine residual risk
- Develop and implement fraud risk response
Consider

- History of fraud in the organization
- Fraud prevalence in the industry
- Ethics and Tone at the Top
- Controls environment
- Organizational complexity
- Resource availability
- Management support of fraud prevention
- Financial anomalies
- Vendor and customer complaints
- Fraud survey results
  - ACFE Report to the Nations

Reporting the Results

- Just the facts
- Tailored to the audience
- Simple and plain
- Enterprise-view
- Focused on what matters
- Clear and measurable actions to reduce fraud
Now what?

- Use the results to
  - Start the fraud dialog going
  - Look for fraud in high-risk areas
  - Hold parties responsible for progress in remediating controls gaps
  - Evaluate Code of Conduct and Ethics Policies
  - Monitor controls
  - Maintain the FRA

Tips (The 5 Keeps)

- Keep it relevant
  - Language (theft, not larceny)
  - Organizational culture and style
  - Organization’s products and processes
- Keep it simple
- Keep it top of mind
- Keep it alive
- Keep it real
Thank you!

W. Noel Haskins–Hafer
Noel_haskins–hafer@intuit.com

Victor Lustig

Appendix

References, samples, etc.
References

- ACFE
  - www.acfe.org
  - Fraud Assessment Toolkit
  - Report to the Nations
- Government of North Dakota
  - www.nd.gov/fiscal/docs/fraudriskdocumentwithappendix.pdf
  - Fraud Risk Assessment form
- IIA
  - www.theiia.org/download.cfm?file-18932
  - Conducting a Fraud Risk Assessment conference session
- IIA, ACFE and AICPA
  - *Managing the Business Risk of Fraud: A Practical Guide*

Sample FRA form

<table>
<thead>
<tr>
<th>Identified Fraud risks and Schemes</th>
<th>Likelihood</th>
<th>Potential Impact</th>
<th>Depth of Controls</th>
<th>Potential Weaknesses</th>
<th>Control Effectiveness Assessment</th>
<th>Risk of Material Misstatement</th>
<th>Risk of Internal Control Deficiency</th>
<th>Risk of Stopping Deficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Reporting</td>
<td>Remote</td>
<td>Low</td>
<td>Weak</td>
<td>Yes</td>
<td>Internal control staff</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Revenue Recognition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expenditure Recognition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overpayments</td>
<td>Low</td>
<td>Medium</td>
<td>Strong</td>
<td>No</td>
<td>Independent staff</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Improper coding of bills</td>
<td>Low</td>
<td>High</td>
<td>Strong</td>
<td>No</td>
<td>Independent staff</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>

Example:

- Identifying risks and schemes
- Assessing likelihood and potential impact
- Evaluating depth of controls and potential weaknesses
- Conducting control effectiveness assessment
- Assessing risks of material misstatement, internal control deficiencies, and stopping deficiencies
FRA form definitions

1. **Identified Fraud Risks and Initiatives**: This column should include a full list of the potential fraud risks and initiatives that may face the organization. This list will be different for different organizations and should be formed by discussions with employees and management and brainstorming sessions.

2. **Likelihood of Occurrence**: To design an efficient fraud risk management program, it is important to assess the likelihood of the identified fraud risks so that the organization establishes proper anti-fraud controls for the risks that are deemed most likely. For purposes of this assessment, it should be adequate to evaluate the likelihood of risks as remote, reasonably possible, and probable.

3. **Significance to the Organization**: Quantitative and qualitative factors should be considered when assessing the significance of fraud risks to an organization. For example, certain fraud risks may only pose an immaterial direct financial risk to the organization, but could greatly impact its reputation, and therefore, would be deemed to be a more significant risk to the organization. For purposes of the assessment, it should be adequate to evaluate the significance of risks as immaterial, significant, and material.

4. **People and/or Department Subject to Risk**: As fraud risks are identified and assessed, it is important to evaluate which people inside and outside the organization are subject to the risk. This knowledge will assist the organization in tailoring its fraud responses, including establishing appropriate segregation of duties, pre-approval and approval chain of authority, and proactive fraud auditing procedures.

5. **Existing Anti-fraud Internal Controls**: Identify existing controls to the relevant fraud risks identified. Note that this occurs after fraud risks are identified and assessed for likelihood and significance. By progressing in this order, this framework intends for the organization to assess identified fraud risks on an as-needed basis, without consideration of internal controls.

6. **Assessment of Internal Controls Effectiveness**: The organization should have a process in place to evaluate whether the identified controls are operating effectively and mitigating fraud risks as intended. Organizations should consider and review what monitoring procedures would be appropriate to implement to gain assurance that their internal control structure is operating as intended.

7. **Remedial Actions**: After consideration of the internal control structure, it may be determined that certain fraud risks may not be mitigated adequately due to several factors, including (a) poorly designed controls are not in place to address certain fraud risk or (b) controls identified are not operating effectively. These residual risks should be evaluated by the organization in the development of the fraud risk response.

8. **Fraud Risk Response**: Residual risks should be evaluated by the organization and fraud risk responses should be addressed such remaining risk. The fraud risk response could be implementing additional controls and/or designing proactive fraud auditing techniques.

Top 10 Internal Control Weaknesses

- Absence of management oversight
- Lack of duty segregation
- Lack of communication
- Absence of account reconciliation
- Poor or outdated information systems
- Weak information security
- Ineffective or incomplete reconciliations
- Absence of analytics
- Absent or weak policies and procedures
- Absent or weak review and approval process