Risk Management and Fraud Mitigation

Thursday, December 12, 2013
8:30 am – 12:00 pm

Presented by:

Marc W. Courey, CPA/CFF, CFE, CICA, CCEP, JD, Director
Risk Management and Fraud Mitigation

Trainer: Marc W. Courey, CPA/CFF, CFE, CICA, CCEP, JD, Director

Agenda

Risk Management (ERM)
- What – is it
- Why – would I do it
- How – do I do it
- Factors that Drive Success
- Benefits of ERM
- What You Can Do to Start ERM Now

Fraud Mitigation
- Background on fraud
- Fraud Risk Assessment
- Internal control opportunities
- Organizational policies (that support better governance)
- Responding to fraud incidents
- Can you solve the puzzle?
Effective ERM programs have these attributes:

- A process driven by senior management and the board of directors to lessen the frequency and impact of potential risks
- Management of risk within a “risk appetite,” using a formal process
- Supports achievement of key strategic objectives and disclosure of risks to primary stakeholders
- Includes all organizational risks; not just financial risks
- Integrates into the daily management process - becoming part of the culture
Common ERM Attributes and Best Practice Result

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Best Practice Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Mindset</td>
<td>Not a once-and done exercise</td>
</tr>
<tr>
<td>Formal Measurement</td>
<td>Integrated and cross-functional portfolio view of risk, no silos, with consideration to both up and downside risks</td>
</tr>
<tr>
<td>Established Scope</td>
<td>All key risks addressed, not just financial (e.g., operational and strategic)</td>
</tr>
<tr>
<td>Program Purpose</td>
<td>Long-term approach to using risk-informed decision making to govern the organization in a way that increase organizational value</td>
</tr>
</tbody>
</table>

Relationship Between ERM, Internal Audit and Other Regulatory Requirements

Although there is overlap, ERM is unique because it provides:

- A broader, higher-level focus on “Enterprise ending risks”
- An opportunity to leverage resources and lessons learned across the organization, while breaking down silos
- Real time, ongoing risk monitoring
- A common risk taxonomy, so risks can be measure, discussed and mitigated “apples-to-apples” across the organization
Enterprise Risk Management

Important Questions ERM Addresses

1. How do I manage the increasing complexity and interdependencies of risk?
2. How do I satisfy the needs of the Board and the Audit Committee?
3. How do I manage the impact of volatility on my financial performance and make the business case for the appropriate amount of spending on risk mitigation?
4. How do I extract value from risk spending while balancing the needs of internal and external stakeholders?
5. How can I reduce fraud risk?
Many Stakeholders are Driving the Need for ERM

**Donors:**
- Trust
- Restrictions

**Auditors:**
- Report risks in a forward-looking context
- Risk-based Auditing (RBA) requirements

**Regulators:**
- Assurance on compliance and financial approval processes

**Families:**
- Quality services for children, etc
- Safety

**Grantors:**
- Financial disclosure
- Transparency
- Compliance

**Watchdogs:**
- Risk disclosure
- Incorporation of ERM criteria into evaluations

Benfits of Establishing an ERM Program

**For Mature Organizations**
- **Fraud Reduction** – reduce and detect fraud
- **Governance** – enhanced and integrated
- **Resource Allocation** – optimized
- **Transparency** – increased risk identification and disclosure
- **Reduced Volatility** – in risk
- **Consistency** – in approach to risk management
- **Regulatory requirements** – Satisfaction of regulatory requirements

**For Growing Organizations**
- **Strategic Plan** – assists in understanding audience and program service risk
- **Raising Funds** – assures lenders, grantors, and donors that risk has been identified and addressed
- **Talent Management & Recruitment** – understand who you need, and how to keep them
- **Support Growth** – manage the uncertainties that a new organization must understand and effectively manage to grow.
Enterprise Risk Management

ERM is a Multi-Step Journey Not a Destination… So Where Should You Start
There is a Roadmap and Critical Path for Successful ERM

1. Identify
2. Assess
3. Respond
4. Monitor and Report
5. Improve

There is a Roadmap and Critical Path for Successful ERM

ERM Foundation
- Culture
- Strategy
- Governance
- Tools
- Education

Successful ERM

Step 1: Develop an ERM Governance Model and Team that Fits Your Organization

Board / Audit Committee

ERM Committee

Internal Audit

Risk Management/Insurance

Compliance

Operations / IT
We’re All Risk Managers

- Account for risk in decision making
- Insurance, investments, hiring, etc.
- Good risk management:
  - Is more structured and organized
  - Involves many (not alone)
  - Is communicated throughout organization
  - Becomes part of the culture

Assemble a Team

- Top management – strategic goals
- Program managers
- Supporting functions
  - Accounting/finance
  - Human resources
  - Information technology
  - Fundraising
  - Legal
  - Building management (if applicable)
Step 2: Identify Risks

- A possible events or circumstances that can have negative influences on the organization
  - Also includes lost opportunities
- Impact on the organization can be in one or more of several areas

Classification of Risks

External
- We have little to no control over whether these events occur or are attempted
- Our goal is to be prepared for them

Internal
- We have much greater control over these risks
Categories of Risk

1. Financial
2. Hazard
3. Compliance
4. Client Service
5. Human Capital
6. Technology
7. Governance
8. Regulatory/Legal

1. Financial Risks

- Loss of income
- Increasing costs
- Going concern
- Liquidity
- Economy
- Federal budget environment
- Investment risks
- Borrowing rates
- Availability of credit
- Inadequate budgeting or planning
- Unreliable accounting records
- Fraud
2. Hazard Risks

- Fire, flood and other losses or impairments of physical assets
- Insurable

3. Compliance Risks

- Noncompliance with laws and regulations
  - Grant-related (Head Start, etc)
  - Non-grant-related (FLSA, FCRA, FACTA, ADA, FMLA, etc.)
  - Federal, state and local (also foreign?)
- Violating terms of contracts
- Compliance with donor restrictions
- Civil wrongs (torts)
4. Client Service Risks

- Harm caused to clients in connection with services we provide
- Theft of client property
- Client identity theft
- Transportation accidents
- Overall satisfaction of clients, program participants
- Changing client needs, desires
- Quality of service
- Breaches of confidentiality

5. Human Capital Risks

- Loss or lack of availability of personnel (employees, volunteers, contractors)
- Loss or lack of availability of specific expertise (e.g. technical skills)
- Leadership; succession
- Diminished morale
- Diminished skills of existing personnel
6. Technology

- Obsolete equipment
  - Leading to inefficiencies or incompatibility
- Access to current technology
- Lack of understanding of technology
- Improper utilization of technology

7. Governance Risks

- Improperly prepared or engaged board of directors
- Inefficient governance practices
- Straying from mission
- Lack of innovation
- Poor strategy
8. Regulation Risks

- New regulations
- New interpretations of existing regulations
- New enforcement efforts regarding regulations

Step 3: Identify Current and Emerging Risks Within Your ERM Scope

Whenever possible, leverage work that has already been performed!

- Surveys
- Interviews
- Workshops
- Peer / Competitor Analysis
- Business Initiatives and Changes
- Fraud Assessment / Prior Frauds
- Annual Risk Assessment
- Previous Audit Results / Open Audit Results
- External Environment
- Information Security Framework (ISF)
- Financial Statement Review
- Review Litigation and Claims
Step 3: (cont.) Measure and Prioritize the Identified Risks Based on Likelihood and Impact

- Risks may impact multiple areas (e.g., financial, legal, regulatory, reputation, personnel) as a result impact may be measured over several factors such as:
  - Financial
  - Loss of key manager
  - National media coverage
- Use both qualitative and quantitative factors to measure likelihood and impact

Factors Affecting Likelihood

- Estimates based on past history or cycles
- Complexity of activities
- Volume of activity or transactions
- Control process effectiveness
- Changing environment or stability
- Overall control environment
Impact/Significance Factors

- Materiality (loss in dollars)
  - Direct and indirect
- Relevance with respect to organization’s mission
- Failure to meet strategic goals
- Reputational issues
- Duration and pervasiveness of the event
- Penalties/sanctions
- Recovery costs
  - Lost time, etc.

Step 3: (cont.) The Final Output of a Risk Assessment is Often a Risk Heat Map

<table>
<thead>
<tr>
<th>Impact</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>Moderate to High</td>
<td>High</td>
</tr>
<tr>
<td>Low</td>
<td>Low to Moderate</td>
</tr>
</tbody>
</table>

- Recruiting and Retaining Top Talent
- Grant noncompliance
- Accident with child
- Volunteer burnout
- Competitor
- Office Safety
- New program integration
- Technology access
- Succession Planning
- Economic downturn
- Fraud
- Currency
Step 4: Determine Your Risk Response Strategy to the Identified and Prioritized Risks

Risk Response Strategies
(Can be used as standalone solutions or in tandem with other solutions)

**Terminate**
- Exit Risk Area

**Mitigate**
- Internal Controls
  - People
  - Process
  - Technology
- Policy & Procedure
- Written Response Plan
- Self Funding (e.g., Reserves and Capital)

**Transfer**
- Insurance
- Contractual Transfer
- Joint Venture
- Hybrid

**Exploit**
- Explore the Upside of Risk by Taking More Risk

**Tolerate**
- Make a Conscience Decision to Tolerate the Risk

Step 5: Monitor, Report On, and Mitigate the Identified Risks

<table>
<thead>
<tr>
<th>Risk</th>
<th>Definition</th>
<th>Current State</th>
<th>Risk Owner(s)</th>
<th>Action Plans</th>
<th>Estimated Cost of Mitigation</th>
</tr>
</thead>
</table>
| Employee Retention | - Ability to recruit and/or retain qualified employees  
- Ability to support growth initiatives  
- Creation of work/life balance for key employees  
- Includes impact of stock option dilution on employee incentive plans | High Impact    | Individual X  
Individual Y | **Always the Organization**  
- Expand upon the existing measurement process to include employee absence costs, turnover and related employee performance metrics  
- Implement an employee retention study to uncover the factors and conditions that impact an employee's decision to remain with the Company. Use the results to develop a formal retention strategy | - $ ### |

Current Metrics:
- Employee engagement metrics
- Total compensation expense
- Time to fill requisitions
- Voluntary and involuntary turnover (regretted and non-regretted)
- Budgets
- Headcount verses growth
- Work/life balance numbers
- Number of job offers rejected

Current State:
- High Impact

Risk Owner(s):
- Individual X
- Individual Y
Step 5: Monitor, Report On, and Mitigate the Identified Risks (cont.)

Summary of ERM Key Concepts

- ERM is a continuous process to identify, measure, manage, and disclose all key risks
- ERM focuses on increasing value to primary stakeholders while satisfying other stakeholders
- ERM has focused resources that improve the organization’s risk identification and management process
- ERM starts with a broad base of risks and prioritize and manages these risks using a process
- ERM is about risk management, not just measurement
Critical Success Factors for ERM

- Senior Management and Board support and involvement
- Leverage existing resources and processes
- Obtain cross-functional representation on the ERM team
- ERM Success

The Return on Your ERM Investment

- Less Risk Events
- Lessen Impact of Risk Events
- Less Fraud
- Better Allocation of Resources
- Increased Organizational Success
Implementing ERM

• Initial Stage
  – Assign responsibility for developing plan to small team
  – Obtain buy-in of key members of management and the board
  – Consideration of plan by full board (perhaps refine the plan)

• Ongoing Stage
  – Begin implementation of plan
  – Embed in various levels of the organization
  – Implement reporting mechanisms
  – Aim for organizational improvement

Integrating ERM

• Most likely failure of ERM is due to lack of integration into ongoing management activities of an organization

• Other limitations of ERM:
  – Breakdowns due to error
  – Collusion
  – Cost vs. benefit
  – Management override
Obstacles to Risk Management

- A board that thinks that risk management is not their issue
- An organizational focus solely on internal financial controls
- Lack of board consensus as to what the organization’s objectives really are
- A view of internal controls as a regulatory exercise
- Risk management is viewed as the responsibility of a single function
- No training on risk awareness for employees

Embed ERM Via:

1. Strategic planning
2. Budgeting
3. Corporate governance
4. Training programs
5. Staff meetings
6. Performance measurement and evaluation
When ERM Works Properly

- It does more than enable the organization to identify risks in a more timely manner and deal with those risks
- It helps to identify opportunities for the organization
- It enhances the strategic, operational, and financial planning processes

Risk Management Best Practices

1. Engaged senior management and board of directors
2. Established ERM framework integrated into ongoing management activities
   - Make it easily repeatable
3. Risk-aware culture via communication, training, incentives, etc.
4. Written policies and procedures
5. Tracking and reporting quantitative risk metrics and qualitative risk assessments
ERM.... Make it Happen Now

Remember, anything is a beginning – start small and build the program by:

- Establishing an ERM governance model
- Performing an enterprise-wide risk assessment
- Considering a risk assessment pilot in a single program or function

Starting the ERM Journey Will Lead to ROI by:

- Keeping your organization out of trouble
- Reducing the cost of risk
- Coordinated risk management activities across the organization (e.g., less redundancy)
- Improving transparency
- Enhancing business processes
- Achieving better return for funding sources and other stakeholders

Closing Thought: Organizations succeed by taking risk and fail by not effectively managing those risks. To succeed you must master risk. To fail you must do nothing.

Background on Fraud
## Background on Fraud

### Industry of Victim Organizations (Sorted by Median Loss)

<table>
<thead>
<tr>
<th>Industry</th>
<th>Number of Cases</th>
<th>Percent of Cases</th>
<th>Median Loss ($)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mining</td>
<td>9</td>
<td>6.7%</td>
<td>$300,000</td>
</tr>
<tr>
<td>Real Estate</td>
<td>36</td>
<td>2.6%</td>
<td>$315,000</td>
</tr>
<tr>
<td>Construction</td>
<td>47</td>
<td>3.4%</td>
<td>$200,000</td>
</tr>
<tr>
<td>Oil and Gas</td>
<td>44</td>
<td>3.2%</td>
<td>$265,000</td>
</tr>
<tr>
<td>Banking and Financial Services</td>
<td>229</td>
<td>16.1%</td>
<td>$220,000</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>139</td>
<td>10.1%</td>
<td>$200,000</td>
</tr>
<tr>
<td>Health Care</td>
<td>52</td>
<td>6.7%</td>
<td>$200,000</td>
</tr>
<tr>
<td>Transportation and Warehousing</td>
<td>36</td>
<td>2.6%</td>
<td>$180,000</td>
</tr>
<tr>
<td>Services (Other)</td>
<td>40</td>
<td>3.6%</td>
<td>$150,000</td>
</tr>
<tr>
<td>Communications and Publishing</td>
<td>9</td>
<td>0.7%</td>
<td>$150,000</td>
</tr>
<tr>
<td>Other</td>
<td>7</td>
<td>0.5%</td>
<td>$150,000</td>
</tr>
<tr>
<td>Telecommunications</td>
<td>43</td>
<td>3.1%</td>
<td>$135,000</td>
</tr>
<tr>
<td>Services (Professional)</td>
<td>55</td>
<td>4.2%</td>
<td>$115,000</td>
</tr>
<tr>
<td>Agriculture, Forestry, Fishing, and Hunting</td>
<td>30</td>
<td>2.2%</td>
<td>$104,000</td>
</tr>
<tr>
<td>Government and Public Administration</td>
<td>141</td>
<td>10.2%</td>
<td>$100,000</td>
</tr>
<tr>
<td>Retail</td>
<td>80</td>
<td>6.1%</td>
<td>$100,000</td>
</tr>
<tr>
<td>Technology</td>
<td>35</td>
<td>2.6%</td>
<td>$100,000</td>
</tr>
<tr>
<td>Insurance</td>
<td>76</td>
<td>5.7%</td>
<td>$86,000</td>
</tr>
<tr>
<td>Religious, Charitable or Social Services</td>
<td>54</td>
<td>3.9%</td>
<td>$85,000</td>
</tr>
<tr>
<td>Arts, Entertainment, and Recreation</td>
<td>32</td>
<td>2.3%</td>
<td>$71,000</td>
</tr>
<tr>
<td>Wholesale Trade</td>
<td>27</td>
<td>2.0%</td>
<td>$50,000</td>
</tr>
<tr>
<td>Utilities</td>
<td>24</td>
<td>1.8%</td>
<td>$26,000</td>
</tr>
<tr>
<td>Education</td>
<td>50</td>
<td>6.4%</td>
<td>$20,000</td>
</tr>
</tbody>
</table>

Source: Association of Certified Fraud Examiners 2010 Report to the Nations

### Background on Fraud

#### Organization Type of Victim – Frequency

<table>
<thead>
<tr>
<th>Type of Victim Organization</th>
<th>2012</th>
<th>2010</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Company</td>
<td>39.3%</td>
<td>42.1%</td>
<td>38.1%</td>
</tr>
<tr>
<td>Public Company</td>
<td>28.0%</td>
<td>33.1%</td>
<td>28.4%</td>
</tr>
<tr>
<td>Government</td>
<td>28.1%</td>
<td>16.3%</td>
<td>19.1%</td>
</tr>
<tr>
<td>Not-for-Profit</td>
<td>10.4%</td>
<td>8.6%</td>
<td>14.3%</td>
</tr>
<tr>
<td>Other*</td>
<td>5.5%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Association of Certified Fraud Examiners 2012 Report to the Nations
Background on Fraud

Size of Victim Organization – Frequency

<table>
<thead>
<tr>
<th>Number of Employees</th>
<th>2012</th>
<th>2010</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;100</td>
<td>31.0%</td>
<td>30.8%</td>
<td>38.2%</td>
</tr>
<tr>
<td>100-999</td>
<td>19.5%</td>
<td>12.8%</td>
<td>20.0%</td>
</tr>
<tr>
<td>1,000-9,999</td>
<td>28.1%</td>
<td>25.9%</td>
<td>23.0%</td>
</tr>
<tr>
<td>10,000+</td>
<td>20.6%</td>
<td>20.6%</td>
<td>18.9%</td>
</tr>
</tbody>
</table>

Source: Association of Certified Fraud Examiners 2012 Report to the Nations

Size of Victim Organization – Median Loss

<table>
<thead>
<tr>
<th>Number of Employees</th>
<th>2012</th>
<th>2010</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;100</td>
<td>$147,000</td>
<td>$155,000</td>
<td>$200,000</td>
</tr>
<tr>
<td>100-999</td>
<td>$150,000</td>
<td>$200,000</td>
<td>$176,000</td>
</tr>
<tr>
<td>1,000-9,999</td>
<td>$100,000</td>
<td>$139,000</td>
<td>$116,000</td>
</tr>
<tr>
<td>10,000+</td>
<td>$140,000</td>
<td>$164,000</td>
<td>$147,000</td>
</tr>
</tbody>
</table>

Source: Association of Certified Fraud Examiners 2012 Report to the Nations
Background on Fraud

**Perpetrator’s Criminal Background**

![Criminal Background Chart]

Source: Association of Certified Fraud Examiners 2012 Report to the Nations

**Perpetrator’s Employment Background**

![Employment Background Chart]

Source: Association of Certified Fraud Examiners 2012 Report to the Nations
Background on Fraud

Occupational Frauds by Category – Frequency*

The sum of percentages in this chart exceeds 100 percent because several cases involved multiple schemes from more than one category.

Source: Association of Certified Fraud Examiners 2012 Report to the Nations

Background on Fraud

Government and Public Administration
141 Cases

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Number of Cases</th>
<th>Percent of Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corruption</td>
<td>50</td>
<td>35.5%</td>
</tr>
<tr>
<td>Billing</td>
<td>33</td>
<td>23.4%</td>
</tr>
<tr>
<td>Non-Cash</td>
<td>27</td>
<td>19.1%</td>
</tr>
<tr>
<td>Skimming</td>
<td>25</td>
<td>17.7%</td>
</tr>
<tr>
<td>Expense Reimbursements</td>
<td>19</td>
<td>13.5%</td>
</tr>
<tr>
<td>Payroll</td>
<td>18</td>
<td>12.8%</td>
</tr>
<tr>
<td>Check Tampering</td>
<td>15</td>
<td>10.6%</td>
</tr>
<tr>
<td>Cash on Hand</td>
<td>12</td>
<td>8.5%</td>
</tr>
<tr>
<td>Cash Larceny</td>
<td>10</td>
<td>7.1%</td>
</tr>
<tr>
<td>Financial Statement Fraud</td>
<td>9</td>
<td>6.4%</td>
</tr>
<tr>
<td>Register Disbursements</td>
<td>4</td>
<td>2.8%</td>
</tr>
</tbody>
</table>

The sum of percentages in this chart exceeds 100 percent because several cases involved multiple schemes from more than one category.

Source: Association of Certified Fraud Examiners 2012 Report to the Nations
### Background on Fraud

#### Education
88 Cases

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Number of Cases</th>
<th>Percent of Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Billing</td>
<td>28</td>
<td>31.8%</td>
</tr>
<tr>
<td>Expense Reimbursements</td>
<td>23</td>
<td>26.1%</td>
</tr>
<tr>
<td>Corruption</td>
<td>21</td>
<td>23.9%</td>
</tr>
<tr>
<td>Skimming</td>
<td>19</td>
<td>21.6%</td>
</tr>
<tr>
<td>Payroll</td>
<td>13</td>
<td>14.8%</td>
</tr>
<tr>
<td>Check Tampering</td>
<td>11</td>
<td>12.5%</td>
</tr>
<tr>
<td>Cash on Hand</td>
<td>11</td>
<td>12.5%</td>
</tr>
<tr>
<td>Cash Larceny</td>
<td>8</td>
<td>9.1%</td>
</tr>
<tr>
<td>Non-Cash</td>
<td>7</td>
<td>8.0%</td>
</tr>
<tr>
<td>Register Disbursements</td>
<td>5</td>
<td>5.7%</td>
</tr>
<tr>
<td>Financial Statement Fraud</td>
<td>4</td>
<td>4.5%</td>
</tr>
</tbody>
</table>

*The sum of percentages in this chart exceeds 100 percent because several cases involved multiple schemes from more than one category.*

Source: Association of Certified Fraud Examiners 2012 Report to the Nations

#### Median Duration – By Fraud Scheme

Source: Association of Certified Fraud Examiners 2012 Report to the Nations
Background on Fraud

**Likelihood individuals will steal:**

- **Will steal:** 30%
- **Might steal:** 30%
- **Won't steal:** 40%


Background on Fraud

**Incentive/Pressures**

**Opportunity**

**Attitude/Rationalization**

**Fraud Overview – Summary**

Understand that:

- Employees will steal
- Fraud occurs in every business
- Privately held companies are more susceptible
  - As are companies with <100 employees
- Most occupational frauds are asset misappropriations
- Most perpetrators have never been charged or convicted
- Most perpetrators have never been punished or terminated

**Fraud Risk Assessment**

“Mini” ERM

- Prioritize what processes will be assessed
  - Consider processes where fraud has previously occurred
  - Consider critical processes that may be more susceptible to fraud
- Identify possible fraud schemes
  - Specific to the prioritized processes selected above
  - Consider any possible abuse unique to each prioritized process
**Fraud Risk Assessment Framework**

Whenever possible, leverage work that has already been performed!

- Surveys
- Interviews
- Workshops
- Peer/competitor analysis
- Business initiatives and changes
- Fraud assessment/prior frauds
- Annual risk assessment
- External business environment
- Information Security Framework (ISF)
- Financial statement review
- Review litigation and claims
- Previous audit results/open audit results

---

**Fraud Risk Assessment Framework**

- Are the Schemes identified likely to occur?
  - What is the possibility of occurrence
  - Assign a “can it happen to us” possibility factor to each scheme
    - Probable
    - Reasonably possible
    - More than remote
    - Remote

- Possibility factor needs to be updated as circumstances change
Fraud Risk Assessment Framework

- Evaluate existing controls and potential loss
- Are the controls currently in place capable of:
  - Preventing
  - Deterring
  - Detecting fraud or abuse
- Determine the effectiveness of each control
- Consider need for additional controls for each potential scheme

Fraud Risk Assessment Framework

- Base the need for additional controls on the impact to your organization’s
  - Reputation
  - Financial stability
- Consider the creation of a “heat map” to better visualize and track the priority issues identified within your organization
If you perform a risk assessment, what should you expect?

- Identification of high risk areas
- List of transactions of interest in high risk areas
- Summary of red flags in those areas
- Plan to detect red flags and mitigate risk

* Source: Fraud Risk Assessments’ Place in ERM by Ronald L. Hagenbaugh. Copyright 2008 by the Institute of Internal Auditors
Internal Control Opportunities

- Policies
- Insurance coverage
- Segregation of duties
- Management review
- Hotline
- Surprise audits/internal audit
- External audit
- Job rotation
- Employee support/assistance programs

Initial Detection of Occupational Frauds

Source: Association of Certified Fraud Examiners 2012 Report to the Nations
Internal Control Opportunities

Frequency of Anti-Fraud Controls

- External Audit of FIS: 70.1% (2012), 70.9% (2010)
- Code of Conduct: 67.3% (2012), 67.5% (2010)
- Management of Certification of FIS: 66.4% (2012), 66.6% (2010)
- Internal Audit/FPL Department: 65.7% (2012), 65.4% (2010)
- External Audit of COSO: 64.1% (2012), 64.0% (2010)
- Management Review: 63.9% (2012)
- Independent Audit Committee: 62.8% (2012)
- Employee Support Programs: 61.8% (2012)
- Hotline: 64.0% (2012)
- Fraud Training for Managers/Executives: 60.7% (2012)
- Fraud Training for Employees: 58.9% (2012)
- Anti-Fraud Policy: 57.5% (2012)
- Formal Fraud Risk Assessments: 55.9% (2012)
- Surplus Audits: 55.5% (2012)
- Job Rotation/Mandatory Vacation: 53.3% (2012)
- Rewards for Whistleblowers: 4.6% (2012)

Source: Association of Certified Fraud Examiners 2012 Report to the Nations

Internal Control Opportunities

Insurance Coverage

- Cost-benefit analysis of employee dishonesty, employee bonding coverage

- Considerations
  - Make a business decision to accept risk of loss
  - Consider how fraud occurs
  - Understand coverage before a loss is incurred

- Key issues
  - Types of coverage to consider
  - Insurance coverage limits and deductibles
  - Any exclusions of coverage
  - Notification requirements for claim
  - Coverage for legal fees and costs of investigation
Internal Control Opportunities

Segregation of Duties

• Authorization
  – Initiation, authorization

• Custody
  – Physical custody

• Recording
  – Recording, reporting

• Establish a process for responding to reports
• Report to senior leadership on reports received

Segregation of Duties (cont.)

• Viable alternatives if not achievable
  – Management review
    • Understand what you’re reviewing
    • Really review it
    • Confirm recording/reporting of what you review
  – Surprise audits
  – Cross training with job rotation
**Internal Control Opportunities**

**Percent of Tips by Source**

- **Employee**: 50.9%
- **Customer**: 22.1%
- **Anonymous**: 12.4%
- **Other**: 11.6%
- **Vendor**: 9.0%
- **Shareholder/Owner**: 2.3%
- **Competitor**: 1.5%

Source: Association of Certified Fraud Examiners 2012 Report to the Nations

---

**Anonymous Reporting Mechanism (“Hotline”)**

- Must be anonymous
- Available 24 x 365
- Not just phone lines
  - Mail
  - Internet
  - Social Networking
- Establish a process for responding to reports
- Report to senior leadership on reports received
## Internal Control Opportunities

### Surprise Audits
- Internal audit
- Preventive as well as detective measure
- Multiple objectives
  - Financial
  - Operational
  - Regulatory
- To be effective
  - Truly must be unscheduled
  - Must be comprehensive (for the area/function being audited)
  - Need trained staff with access
  - Can be outsourced, co-sourced or internally staffed

### External Audits
- Financial reporting
- Regulatory requirements
- Not very effective for identifying fraud
  - Tend to be regularly scheduled
  - Focused on materiality
  - Financial Statements not materially misstated
Internal Control Opportunities

Miscellaneous opportunities

- Mandatory vacations
- Employee background and/or credit checks
  - Pre-employment
  - Ongoing
- Employee Assistance/Support Programs

And finally, remember that **TRUST** is NOT an internal control.
### Organizational Policies

- Ethics statement
- Fraud policy
- Harassment/discrimination
- Acceptable use/expectation of privacy
- Conflict of interest
  - Disclosures
- Obligation to cooperation with investigations
- Background checks
- Communicated to staff, stakeholders, clients
  - Frequency, importance
- Training for staff on policies

### Fraud Policy

**Definition**
- Written procedures to address a suspected fraud incident

**Purpose**
- Communicate process and responsibilities
- Action plan developed before an incident occurs

**Content**
- Examples of fraudulent activities
- Process and responsibilities for reporting, responding to, and investigating suspected fraud activity
- Consequences and corrective actions for violations
- Signature of employee
### Organizational Policies

#### Ethics Policy
- **Definition**
  - Focused statement of ethical standards of organization
- **Purpose**
  - Communicate organization expectations
  - Provide guidance to address ethical questions
- **Content**
  - Summary of ethical values of organization
  - Statement of expectation for ethical conduct
  - Descriptions of unethical conduct
  - Signature of employee

#### Fraud Response
- **Definition**
  - Written procedures to address a suspected or actual fraud incident
- **Purpose**
  - Communicate process and responsibilities
  - Action plan developed before an incident occurs
- **Content**
  - Examples of fraudulent activities
  - Process and responsibilities for reporting, responding to, and investigating suspected or actual fraud activity
  - Consequences and corrective actions for violations
  - Signature of employee
Organizational Policies

Conflict of Interest Disclosures

• Definition
  – Report of business relationships that could potentially result in a conflict of interest

• Purpose
  – Document business affiliations and interests
  – Provide a mechanism for disclosing and clearing conflicting relationships
  – Provide opportunity for secondary review

• Content
  – Lists of business ownership and investments
  – Explanation of potential conflict of interest
  – Explanation of process to approve relationships
  – Signature of employee

Organizational Policies

Duty to Cooperate

• Definition
  – Requires employees to cooperate with the organization in the course of an investigation

• Purpose
  – Communicates the expectation of ethical conduct
  – Allows discipline, up to and including discharge, for a failure to cooperate
  – Provides staff with an “out” during an investigation

• Content
  – The organization expects, and staff agree, to cooperate
  – With any legal requests made
  – By the organization or its representatives
  – In the course of an investigation
Responding to Fraud Incidents

• Should an organization always investigate suspected fraud?
• What are the pros and cons of investigating suspected fraud?

Advance planning for appropriate fraud response is essential.
Organizations must be able to:
• Respond to reports of suspected fraud
• Respond to discovery of actual fraud

It’s not a matter of if fraud will occur, but when. Consider that fraud may be happening now.
Responding to Fraud Incidents

Incidents of fraud can impact an organization and disrupt its operations just as severely as commonly planned for critical events such as fires, floods, and other disasters.

- Potential Impacts
  - Loss of assets
  - Damage to reputation
  - Loss of funding, client, stakeholder trust
  - Litigation
  - Failure of organization

While many organizations are making fraud prevention and detection a priority through the implementation of anti-fraud controls, even the best control systems cannot eliminate the risk of fraud.

- An organization may have a duty and responsibility to investigate and resolve allegations of fraud.
  - Statutory requirements
  - Common law requirements
- Directors and managers may have a personal responsibility to ensure fraud is investigated.
- Statutory requirements
  - Sarbanes-Oxley: §§ 301, 302, 404, 906
  - Foreign Corrupt Practice Act of 1977 (FCPA)
  - Anti-Kickback Act of 1986
  - Other federal and state laws requiring the preparation and filing of accurate financial statements and public reports
- Duties of reasonable care and loyalty
  - Responsibility to use same reasonable care in conducting affairs of organization as used in conduct of personal affairs
  - Directors and officers with fiduciary responsibilities
Responding to Fraud Incidents

What risks can arise from the conduct of a fraud investigation?

- Criminal and civil liability for fraud
  - Liability for organization’s actions
  - Liability for employees’ actions
- Public disclosure of fraud
- Public disclosure of sensitive information
- Mismanaged investigations
  - Legal action by employees
    - Invasion of privacy
    - Intentional infliction of emotional distress
    - Defamation
    - Breach of good faith and fair dealing
    - Breach of implied contract
    - False imprisonment
    - Trespass
  - Violation of Electronic Communications Privacy Act of 1986
    - Interception of wire, oral or electronic communications
    - Access to employees’ e-mail and voice mail
  - Increase the risk of criminal, regulatory or civil sanctions
Responding to Fraud Incidents

Which key people should participate in fraud response?

- What is their role?
- Why?

The Fraud Response Team

- No single person can effectively address every issue arising during a fraud investigation.
- Identify key people and define their responsibilities before a fraud occurs
  - Legal counsel – internal/external
  - Executive Director/management representative
  - Fraud investigator – Certified Fraud Examiner/Forensic Accountant
  - Computer forensic specialist/consultant
  - Internal auditors
  - IT/system administrators
  - Security staff
  - Human resources
  - Public relations
## Responding to Fraud Incidents

- Fraud response plan outlines the actions your organization will take when potential fraud has been identified
- Do not attempt to define how an actual investigation will be conducted
  - Rely on legal counsel and experienced fraud investigators to conduct investigation
- Focus fraud response planning on managing the organization’s overall actions
  - Help create conditions for successful investigation
  - Help manage associated risks

## Responding to Fraud Incidents

What elements should be included in a fraud response plan? Why?
Responding to Fraud Incidents

- Confirm predication of fraud
  - Totality of circumstances that would lead a reasonable, professionally trained and prudent individual that fraud has occurred
  - Consider alternative actions if predication is not confirmed
- Engage legal counsel
  - Engage legal counsel, Engage legal counsel, Engage legal counsel
- Activate fraud response plan/team
- Determine potential impact
  - Financial – estimate loss from fraud
  - Regulatory – impact on programs, notification
  - Other impacts – reputational, loss of funding
  - Cost of effective fraud investigation and response

Responding to Fraud Incidents

- Determine the objectives of fraud response
  - Find out what happened
  - Discipline/prosecute fraudsters
  - Protect organization’s reputation
  - Recover lost assets
  - Minimize risk of litigation or prosecution of organization
- Develop communication strategy
  - Legal or regulatory reporting obligations
  - Communications with company management
  - Balance investigative considerations with employee needs
  - Manage communications to external audiences
Responding to Fraud Incidents

- Employee privacy expectations in workplace
  - Right to search work areas and personal belongings
  - Right to monitor and retrieve all electronic communications conducted via company systems

- Disciplinary policies and procedures
  - Define actions to be taken against employees committing fraud
  - Requirement for employees to cooperate with investigations
  - May help strengthen “Tone at the Top”
  - May help minimize some legal risks

- Ongoing communication of policies and procedures to employees critical to their effectiveness

Can You Solve the Puzzle?

- Working Groups
  - Fraud risk assessment
  - Internal control opportunities
  - Organizational policies
  - Fraud response

- Questions
Can You Solve the Puzzle?

• Split up into groups
  – Determine appropriate path for your organization
    • Each group has a different fact scenario
    • You are the Board, senior leadership
    • Consider your objectives and environment
    • Report to the group/group discussion
      – What you decided was appropriate under the circumstances
      – Why you decided the course for your organization

Can You Solve the Puzzle?

• Issue 1: Fraud risk assessment
  – Prioritize fraud risks to your organization

• Issue 2: Internal control opportunities
  – Identify specific internal controls and activities

• Issue 3: Organizational policies
  – Policies your organization will adopt & implement

• Issue 4: Fraud response
  – Your organization believes it has a problem – what do you do now?
Can You Solve the Puzzle?

• Split into working groups
  – Spend 5 minutes reviewing your fact scenario
  – Select your reporter
    • Different reporter for each issue
  – Conduct your fraud risk assessment
Issue #1

- Fraud risk assessments
  - Risk areas
  - Why
Issue #2

- Internal control opportunities
  - Identify specific internal control activities your organization will implement.
  - Why?
Issue #3

- Organizational policies
  - Specific policies you will adopt and implement
  - Why?
Issue #4

- You think you have a problem?
  - What do you do now?
  - Why?

Additional Resources

<table>
<thead>
<tr>
<th>Resources</th>
<th>Websites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Association of Certified Fraud Examiners</td>
<td><a href="http://www.acfe.com">www.acfe.com</a></td>
</tr>
<tr>
<td>Transparency International (Corruption Perception Index)</td>
<td><a href="http://www.transparency.org">www.transparency.org</a></td>
</tr>
<tr>
<td>The Institute of Internal Auditors</td>
<td><a href="http://www.theiia.org">www.theiia.org</a></td>
</tr>
<tr>
<td>Open Compliance and Ethics Group</td>
<td><a href="http://www.oceg.org">www.oceg.org</a></td>
</tr>
<tr>
<td>International Association of Financial Crimes Investigators</td>
<td><a href="http://www.iafci.org">www.iafci.org</a></td>
</tr>
<tr>
<td>Society of Corporate Compliance and Ethics</td>
<td><a href="http://www.corporatecompliance.org">www.corporatecompliance.org</a></td>
</tr>
<tr>
<td>American Institute of Certified Public Accountants – Forensic and Valuation Services</td>
<td><a href="http://www.fvs.aicpa.org">www.fvs.aicpa.org</a></td>
</tr>
</tbody>
</table>
### Additional Resources

<table>
<thead>
<tr>
<th>Resources</th>
<th>Websites</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Committee of Sponsoring Organizations of the Treadway Commission (COSO)</td>
<td><a href="http://www.coso.org">www.coso.org</a></td>
</tr>
<tr>
<td>Chartered Institute of Management Accountants</td>
<td><a href="http://www.cimaglobal.com">www.cimaglobal.com</a></td>
</tr>
<tr>
<td>ASIS International</td>
<td><a href="http://www.asisonline.org">www.asisonline.org</a></td>
</tr>
<tr>
<td>The Serious Fraud Office (UK)</td>
<td><a href="http://www.sfo.gov.uk">www.sfo.gov.uk</a></td>
</tr>
<tr>
<td>Information Systems Audit and Control Association</td>
<td><a href="http://www.isaca.org">www.isaca.org</a></td>
</tr>
<tr>
<td>U. S. Department of Justice</td>
<td><a href="http://www.usdoj.gov">www.usdoj.gov</a></td>
</tr>
</tbody>
</table>
## How We Can Help

### Risk

#### Consulting
- Internal Controls Review
- Risk Assessments
- Fraud Prevention
- Anti-Corruption Services
- Litigation Readiness
- Electronic Data Analysis
- Fraud Investigations
- Digital Forensics

#### Training
- On-Site Training
- Webinars

#### Audit
- Financial statement audits
- Single audits (A-133)
- Program-specific audits
- Financial statement reviews and compilations
- Employee benefit plan audits
- Agreed-upon procedures

### Products
- Finance, HR, and Technology Policy and Procedure Templates (ProPackage)
- My Wipfli Membership Service

---

## For More Information on How We Can Help

Visit with **Wipfli** during the Embassy Suites Manager’s Reception tonight at 5:30 p.m. in the hotel lobby.
**Evaluation!**

Please turn in your evaluation as you leave. We love your feedback!

Thank You!

Presenter Info:

Marc W. Courey, CPA/CFF, CFE, CICA, CCEP, JD, Director
mcourey@wipfli.com
952.548.3439
Reference Materials

Organization Scenarios ........................................ 1
Scenario #1

Southeast Head Start, Inc. runs a stand-alone Head Start agency that covers 5 counties in a moderately populated area. Their Head Start grant is $3,500,000 a year with an additional $300,000 in Child and Adult Care Food Program to feed the children in the program. They have approximately 500 children enrolled in the program and receive no state funding with only about $50,000 a year in outside donations. They have a Finance Director along with one other person in the accounting department. They have an Executive Director a HR Director, a person responsible for IT (among his many responsibilities) and one Program Director. Their fiscal year end is the same as the Head Start grant year end. They have a 12 person Board of Directors, some members of which are involved in the internal controls process (by reviewing and signing checks).

The organization has been in existence for over 30 years, with Board members tenure ranging from 8 to 15 years. The Executive Director, Finance Director, and Program Director are all new to the organization, and Head Start programs, within the past two years. They, along with the Board, rely heavily on the supporting staff in performing their duties for the organization. The Board is concerned about program staffing levels and service delivery next year in light of operating deficits experienced during the past two years.
Scenario #2

Council for Children runs a stand-alone Head Start agency that covers 1 county in an urban environment. Their Head Start grant is $25,000,000 a year with an additional $2,000,000 in Child and Adult Care Food Program to feed the children in the program. They have approximately 5,000 children enrolled in the program and receive an additional $5,000,000 in state funding to serve another 1,000 children. They have about $250,000 a year in outside donations. They contract with 5 separate, unrelated not for profits that Council for Children delegates the delivery of Head Start services to for approximately 2,000 children. To monitor these delegate agencies, Council for Children has a Compliance Officer who has a staff of 2. They have a Chief Finance Officer along with 4 other people in the accounting department. They have an Executive Director, a HR office and an IT department and a program director. Their fiscal year end is the same as the Head Start grant year end. They have a 15 person Board of Directors who are not involved in the day to day internal controls, but who approve the annual budget and review financial reports.

Except for the Chair (who has been with the Council for 13 years), other Board members have been with the organization for from 1 to 5 years. Current staff policies, at least those that exist, were last reviewed in 1999. For years the organization had served approximately 2,000 children, but demand for the services have expanded significantly during the economic downturn began three years ago. Staffing has increased rapidly over the past three years, with office staff having been with the Council for 2.7 years. Additionally, they are projecting that demographics in the community will grow the children in the area needing services from the 6,000 currently served to approximately 8,200 in two years. The Board Chair has been approached by a neighboring agency that is struggling to serve those in its geographic region after suffering significant operating shortfalls the past two years. The Board is concerned about successfully serving all the families in need of the services, and is looking to manage the resources and staff in the coming years.
Scenario #3

Rural CAP has $15,000,000 a year in annual grant revenue. They operate 10 different programs from Head Start, Rural Transportation, Senior Dining, WIC, Weatherization and Energy Assistance. Their largest program is the Energy Assistance Program with $6,000,000 a year in revenue. They have an additional four grants that are state or county funded and receive about $1,000,000 a year in private donations. They have a Fiscal Director along with 3 other people in the accounting department. They have an Executive Director, an HR Director, an IT Director and program directors for each of the large programs. They have grants that end 7 of the 12 months of the year and their fiscal year end is December, which coincides with their largest grant's end date. They have a 17 person Board of Directors who are not involved in the day to day internal controls, but who approve the annual budget and review financial reports.

R-CAP has seen a 44% increase in the number of applications from program participants during the same time there has been a 15% decrease in the amount of grants from government sources. Two methods the Board has used to manage the organization during the strain on program dollars have been a freeze on staff compensation and 25% decrease in staffing levels. Some similar nearby organizations have seen their programs suffer from fraudulent participants with the result that their funding has been significantly reduced, or they are operating under significant governmental oversight, or both. Early applications for the coming programs indicate a significant increase in prospective participants again, and funding sources are already asking how R-CAP can show that they have not allowed ineligible participants (as was uncovered in the neighboring programs)?
Scenario #4

Southern Area Agency on Aging is a pass thru agency for the Senior Nutrition grant (Meal on Wheels and Congregate Dining). They are located in a large municipality and receive $9,000,000 a year in revenue from the State Board on Aging, who receives it from the Federal Government. S3A passes thru 80% of the money they receive to 8 other agencies that actually provide the services to the seniors. S3A does not perform any of the meal services themselves, but does run a Senior Assistance phone hotline for seniors to call. S3A keeps about 10% of the grant as an administrative charge. They have 2 people in the finance department, an Executive Director and 4 compliance officers who monitor the agencies that contract with S3A to perform the services. S3A has a 21 person Board of Directors, at least 12 of which are required to be on the Board due to their position as county commissioners.

Over the past 4 years S3A has used 13 different agencies to provide its services. The Paper of the Free World recently ran an investigative reporting series which documented how NorthWest Area Aging Agency, located in North West County, had been utilizing subcontractors who were not properly licensed, and apparently had been using the meal services to conceal their primary business in a variety of criminal activities. S3A leadership has assured the Board that that “could never happen here.”
Scenario #5

Housing Specialist, Inc. is a $2,000,000 to $7,000,000 a year housing organization, depending on the year. They operate approximately 50 low-income housing complexes and receive HOME and Neighborhood Stabilization Program revenue periodically to purchase and rehab other low-income housing projects, utilizing a combination of staff and subcontractors. They have apartment complexes all over their state, but the administration function is located in once city. They have a President and a CFO along with 4 people in the accounting function. They receive thousands of checks each month from tenants paying their rent, but only receive a handful of deposits each year from gov’t sources. They do not have an IT person but do have an HR Director. They have a 6 person Board of Directors, which meets four times a year. The President of HIS founded the organization 25 years ago and uses his strong personality as the main driver of the organization.

As a new member of the board, you have been unable to get documentation that would allow you to understand where all the properties are, who all the tenants are, and the debt owed on all the housing complexes. Additionally, you have located only scattered policies and procedure manuals regarding personnel and financial policies. Your inquiries of staff regarding selection of subcontractors for rehab work are met with “the President handles all that.”
Scenario #6

The Wisconsin Chapter of Fraternal Fraud Fighters (WIFFF) is organized as a §501(c)6 not-for-profit. Its membership is open to individuals, and may or may not be members of FFF international. WIFFF receives virtually all of its financial backing either from the annual membership fee (currently $35/year) or the fee charged to attend its quarterly networking and training sessions (between $25 and $40). It currently has approximately 120 members (membership has ranged from 40 to 120 members over the past five years) and averages 110 attendees at the quarterly meetings. The volunteer Board is currently composed of 11 members, including the organization’s four officers, and meets in person following each quarterly meeting and telephonically each month between meetings. Finances are handled almost exclusively by the Treasurer, even though the President (also Board Chair) and Vice President are also signers on the financial accounts.

The current officers (except for the Treasurer) have all served in their current capacity for 5 to 9 years. Other board members have been active participants for two years or less. Current membership (1 month into the new fiscal year) stands at 125 members, the highest level anyone can recall.