SEC 210: Fraud Detection and Prevention
Introduction

Donald R. Owens
Shareholder
Internal Audit and Risk Advisory Services
CPA, CFF, CIA, CFSA, CRMA, CBA

Schneider Downs & Co., Inc.
41 S. High Street
Suite 2100
Columbus, OH 43215

Email: dowens@schneiderdowns.com
Work Phone: (614) 586-7257
Cell Phone: (614) 271-8551
Fax: (614) 621-4062
Disclaimers

IRS CIRCULAR 230 DISCLOSURE: Any tax advice contained in this communication (or in any attachment) is not included or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code, or (ii) for promoting, marketing or recommending to another party any transaction or other matter addressed in this communication (or in any attachment).

The views expressed by the presenter do not necessarily represent the views, positions, or opinions of Schneider Downs & Co., Inc. These materials, and the oral presentation accompanying them, are for educational purposes only and do not constitute accounting, tax or legal advice or create an accountant-client or attorney-client relationship.
Fraud

Strange new trend at the office. People putting names on food in the company fridge. Today I had a tuna sandwich named Kevin.
Presentation Take-Aways

- Recognizing and assessing fraud threats in your environment
- How to effectively design and conduct fraud risk assessment
- Evaluating factors that contributed to frauds
Recognize A Threat
Recognize A Threat
Recognize A Threat
Fraud and Its Faces

- Deliberate deception to secure unfair or unlawful gain
- Intentional deception of a person or entity by another made for monetary or personal gain
- Intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right
“Fraud and stupidity look an awful lot alike.”

- Alan Bachman, CFE, MBA
  Education Manager at ACFE
Government fraud refers to illegal acts that intentionally divest the government of funds through deception or scams.

When the government gets swindled, taxpayers pay the price.
“There is no kind of dishonesty into which otherwise good people more easily and more frequently fall than that of defrauding the government.”

- Benjamin Franklin
Public Corruption – “It’s our top priority among criminal investigations” - FBI

Public corruption poses a fundamental threat to our national security and way of life. It impacts everything from how well our borders are secured and our neighborhoods protected... to verdicts handed down in courts... to the quality of our roads, schools, and other government services. And it takes a significant toll on our pocketbooks, wasting billions in tax dollars every year.
Agenda

• Fraud
  ➢ Types of Fraud
  ➢ Basics of Fraud
  ➢ Statistics
  ➢ Red Flags
  ➢ Prevention
• Fraud Risk Assessment
• Internal Controls
• Whistleblower Program
• Resources
# Types of Fraud

<table>
<thead>
<tr>
<th>Fraudulent Financial Reporting</th>
<th>Misappropriation of Assets</th>
<th>Corruption</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Revenues</td>
<td>• Cash theft</td>
<td>• Bribery</td>
</tr>
<tr>
<td>• Expenses</td>
<td>• Fraudulent disbursements</td>
<td>• Bid rigging/Kickbacks</td>
</tr>
<tr>
<td>• Improper valuation or misclassification</td>
<td>• Payroll fraud</td>
<td>• Illegal payments</td>
</tr>
<tr>
<td></td>
<td>• Expense reimbursement</td>
<td>• Conflicts of interest</td>
</tr>
<tr>
<td></td>
<td>• Capital assets/inventory</td>
<td>• Aiding and abetting fraud</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(money laundering)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Almost always material - directly impacts the financials</th>
<th>May or may not be material - directly impacts financials</th>
<th>May or may not be material - indirectly impacts the financials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almost always involves senior management</td>
<td>Can involve any level of employee</td>
<td>Can involve any level of employee</td>
</tr>
<tr>
<td>Controls are less effective in preventing and detecting fraud</td>
<td>Controls can be effective, particularly with regard to those below top management</td>
<td>Controls can be difficult and expensive to implement. Requires close scrutiny of employee activities and cost to do business</td>
</tr>
</tbody>
</table>
## Types of Fraud

<table>
<thead>
<tr>
<th>Theft of Sensitive Data</th>
<th>Defrauding Customers</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Customer and employee personal information</td>
<td>• Intentionally misrepresenting products and services</td>
<td>• Undocumented employees</td>
</tr>
<tr>
<td>• Proprietary information/trade secrets</td>
<td>• Inflating invoices/duplicate billings</td>
<td>• Unrecorded wages</td>
</tr>
<tr>
<td>• Patents, copyrights, other legally protected intellectual property</td>
<td>• Shorting orders/product</td>
<td>• Unreported accidents</td>
</tr>
</tbody>
</table>

May or may not be material/measurable - indirectly impacts the financials

May or may not be material - directly impacts financials

May or may not be material - indirectly impacts the financials

Can involve any level of employee

Can involve any level of employee

Can involve any level of employee

Controls can be difficult and expensive to implement

Controls can be effective, particularly with regard to those below top management

Controls can be effective at all levels
Types of Fraud

Key Areas of Concern
- Credit and Debit cards
- Corruption
- Billings
- Cash theft
- Payroll
- Personal expenses
- Third Party Vendors
- Related Parties
Basics of Fraud

Know that...

- Fraudsters are creative
- Fraudsters appear trustworthy
- Fraudsters are long-standing reliable employees
- Fraudsters are active members of the community
- Fraudsters are sitting in cubicles near you
- Fraudsters are becoming more tech-savvy
Basics of Fraud

“Most occupational fraudsters are first-time offenders. Only 5.2% of perpetrators in this study had previously been convicted of a fraud-related offense, and only 8.3% had previously been fired by an employer for fraud related conduct.”

Source: ACFE Report to the Nations on Occupational Fraud and Abuse (2016)
Basics of Fraud

Fraud or Not

- Bookkeeper removes cash from agency’s for personal use
- Finance Director withdraws funds from operating and payroll accounts then creates unsupported receivable entries to balance the records and conceal the action
- Risk Manager receives lucrative gifts from vendors
- Procurement Manager directs payment to his accounts
- Executive uses agencies assets for personal business
Basics of Fraud

The Fraud Triangle

Rationalization
(Justification of Act)

Need/Pressure
(Influences/Motivation)

Opportunity
(access/entry to the asset)

“Process and Controls”
Basics of Fraud

The Fraud Diamond/Rectangle

- Incentive
  (Influences/Motivation)
- Opportunity
  (access/entry)
- Rationalization
  (Justification of Act)
- Capability
  (Competency to execute)

FIGURE 4: The Fraud Diamond

SEC 200: Fraud Detection and Prevention
Basics of Fraud

• An organization CANNOT control a fraudster’s need and rationalization for his/her actions

• An organization CAN control the opportunities for the fraudster to commit the crime

• Consider the capabilities of employees to commit the crime (competence to execute)
Basics of Fraud

Escalation Fraud Theory
Basics of Fraud

Consequences

- Loss of assets
- Destroyed reputation (both entity AND the individual)
- Job loss
- Civil lawsuits
- Criminal prosecution
Fraud Statistics

Sources of Detection

Figure 22: Detection Method by Size of Victim Organization

Source: ACFE Report to the Nations on Occupational Fraud and Abuse (2016)
Fraud Statistics

Figure 21: Initial Detection of Occupational Frauds

Source: ACFE Report to the Nations on Occupational Fraud and Abuse (2016)
Figure 43: Industry of Victim Organizations

Source: ACFE Report to the Nations on Occupational Fraud and Abuse (2016)
Fraud Statistics

Figure 65: Position of Perpetrator—Frequency and Median Loss

Source: ACFE Report to the Nations on Occupational Fraud and Abuse (2016)
Fraud

Just completed a course on fraud detection and prevention.

Was it valuable?

Valuable—Absolutely, I’ve never made such easy money!
Ethics and Fraud are so inter-connected. Without a strong ethical culture, fraud risk exponentially increases.

In most fraud cases uncovered, indicators that a fraud was occurring were evident to others. However, human nature is to continue to trust those around us even when faced with evidence to the contrary.

**Misplaced Trust is a Great Facilitator of Fraud**
Fraud Red Flags

Fraud Opportunity

Employee’s years of service

Number of key responsibilities residing with the employee

Organization’s complacency level with respect to validating controls and monitoring activities

= Potential for fraud to be committed
Fraud Red Flags

Employee Habits

- Lifestyle or behavior changes
- Personal debt or credit problems
- Refusal to take vacation or sick leave
- Excessive overtime
- Does not produce information voluntarily
- Volatile, arrogant, confrontational or aggressive when challenged
- Indignant with respect to training a back-up
Fraud Red Flags

Management

- Reluctance to provide information
- Dominates all decisions
- Overrides internal controls
- High employee turnover
- Unusual transactions made outside of the system
- Exhibits unusual stress
- Retains excessive authorities and duties (Lack of segregation)
Fraud Red Flags

**Accounting/Operational Indicators**

- Large number of write-offs
- Discrepancies between bank deposits and postings/book
- Excessive/unjustified cash adjusting entries
- Incomplete/untimely bank reconciliations
- Lack of support for transactions
- Missing or presumed misplaced equipment
Fraud Red Flags

Cash Receipts and Disbursements

• Receives, posts and deposits payments (Lack of segregation of key duties)
  ➢ Physical/Manual Duties
  ➢ System Capabilities

• Missing deposits
• Absence of a cash receipt log
• Lack of controls over management signature
• Uncontrolled access to blank checks
Fraud Red Flags

Purchasing

• Able to establish vendors and process invoices (Lack of segregation of key duties)
• Excessive/unusual exceptions to purchasing policies
• Uncontrolled access to the vendor master file
• Vendors with employee names/addresses
• Duplicate purchase orders
• Copies of invoices used to pay vendors
• Less than arms-length transactions and conflicts of interest
• Undue influence
Fraud Red Flags

Fixed Assets

• Authorizes purchases, records FAs, performs write downs assets (lack of segregation of key duties)
• Lack of periodic inventory of assets
• Lack of asset tags/tracking
• Lack of physical security
Fraud Prevention

MAIN TAKE-AWAY

“Awareness”
Fraud Prevention

Practices to Consider

• Adequate resources
• Robust hiring practices
• Periodic audits/reviews
• Conflicts of interest policies and practices
• Insist on adequate documentation
• Tone at the top
• Open door policy
• Culture of compliance and ethics
• On-going and required anti-fraud training
• Fraud reporting tool (hotline)
• Fraud risk assessments
• Strong internal controls
Fraud Risk Assessment

- Develop a FRA Framework
- Populate fraud risks
- Rate probability and impact
- Identify controls and assess alignment
- Identify gaps
- Remediation

SEC 210: Fraud Detection and Prevention
Fraud Risk Assessment

Identify the Opportunities to Commit Fraud

• Create a profile that includes a list of the different areas in which fraud may occur and the types of fraud that are possible in each area (brainstorming, analysis of prior frauds, public information/Google alerts)

• Consider the various types of schemes and scenarios that could occur within an organization

• Don’t overlook information technology impact (enabler or deterrent)
Fraud Risk Assessment

Measuring Fraud Risk

Probability/Likelihood

Prior instances, prevalence, and other factors, including volume of transactions and complexity, and number of people involved in the process should be considered

- Remote
- Reasonably possible
- Probable
Fraud Risk Assessment

Factors to Measure Probability

- Controls or lack of
- Integrity of the organization
- Organizational downsizing
- Budgets decreasing
- Organization doing more with less
- Stressed and disgruntled employees
Fraud Risk Assessment

Measuring Fraud Risk

Impact/Severity

Should include financial, monetary, operational, reputational as well as criminal, civil and regulatory liability considerations

• High
• Moderate
• Low
Fraud Risk Assessment

Other Measures to Consider

• Velocity/speed
• Frequency/persistence
• Direction of fraud risk
**Fraud Risk Assessment**

<table>
<thead>
<tr>
<th>Type of Fraud</th>
<th>Fraud Risk Number</th>
<th>Risk</th>
<th>Examples of Threat</th>
<th>Potential Impact (high – moderate – low: 6-3-1)</th>
<th>Factors Considered to Enhance Potential Impact Rating</th>
<th>Probability of Fraud Occurrence (high – moderate – low: 6-3-1)</th>
<th>Factors Considered to Enhance Probability of Fraud Occurrence (high – moderate – low: 6-3-1)</th>
<th>Combined Internal Fraud Measurement Score</th>
<th>Control(s) to Mitigate Interest Risk</th>
<th>Control Supportive Remuneration</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Fraudulent Financial Reporting (FSR)</td>
<td>1.1</td>
<td>Scheme application of GAAP by corporations (alleged)</td>
<td>Gross misrepresentations in financial reporting (alleged), fraud (alleged), misrepresentations in financial reporting (alleged), revenue recognition (misstatement), liabilities (misstated).</td>
<td>3</td>
<td>3</td>
<td>8</td>
<td>HIGH-RISK</td>
<td>Asset Control 1</td>
<td>Rely on: Observation 4000, QTR 4 - week XXX.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.2</td>
<td>Imprecise top-coded entries</td>
<td>Manipulation of financial performance</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>MEDIUM-RISK</td>
<td>Asset Control 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.3</td>
<td>Timing differences</td>
<td>Revenue recognition in financial period, lower liabilities recognized at month-end</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>LOW-RISK</td>
<td>Asset Control 3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.4</td>
<td>Improper accounting estimates or reserves</td>
<td>Manipulation of financial performance, underestimates of contingent liabilities</td>
<td>3</td>
<td>3</td>
<td>8</td>
<td>HIGH-RISK</td>
<td>Asset Control 4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.5</td>
<td>Delinquent or inaccurate tax liabilities</td>
<td>Underestimation of liabilities, fraudulent tax reporting</td>
<td>5</td>
<td>3</td>
<td>8</td>
<td>HIGH-RISK</td>
<td>Asset Control 5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.6</td>
<td>Incompetency of personnel, unqualified personnel</td>
<td>Sign-off or representation not made; representations made up or inflated without consideration of transactions, accounting, financial control, valuation standards, benefits of delay</td>
<td>3</td>
<td>3</td>
<td>8</td>
<td>HIGH-RISK</td>
<td>Asset Control 6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2) Theft/theft of company property (FT)</td>
<td>2.1</td>
<td>Manipulation of cash</td>
<td>Person or disguised employee gains access to systems in an effort to steal data</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>MEDIUM-RISK</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.2</td>
<td>Software development/computer records</td>
<td>Removal or destruction of information relating to accounting information, thefts of personal performance in an effort to later discovery of facts</td>
<td>3</td>
<td>3</td>
<td>8</td>
<td>HIGH-RISK</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.3</td>
<td>Computer hacking</td>
<td>Unauthorized access to retrieve system records</td>
<td>3</td>
<td>2</td>
<td>8</td>
<td>HIGH-RISK</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.4</td>
<td>Theft of proprietary/confidential information</td>
<td>Use of company assets for personal gain</td>
<td>5</td>
<td>3</td>
<td>8</td>
<td>HIGH-RISK</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.5</td>
<td>Theft contra theft</td>
<td>Obtain travel funds for personal benefit, personal gain</td>
<td>5</td>
<td>3</td>
<td>8</td>
<td>HIGH-RISK</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3) Defrauding Customers</td>
<td>3.1</td>
<td>Counterfeit</td>
<td>Use of services with no intent to pay</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>LOW-RISK</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.2</td>
<td>Intentional sale of substandard products/services</td>
<td>Bulk negotiations to take advantage of price variations, breach confidentiality, manipulation of control dependability requirements</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>LOW-RISK</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4) Misappropriation of Assets</td>
<td>4.1</td>
<td>Embezzlement</td>
<td>Cash handling, forgery, stealing, undeclared cash</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>LOW-RISK</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4.2</td>
<td>Vendor abuse</td>
<td>Improper payment, false accounts payable</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>LOW-RISK</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4.3</td>
<td>Asset theft</td>
<td>Unauthorized theft, theft from the product shortage</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>LOW-RISK</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4.4</td>
<td>Deception of duties opportunities</td>
<td>Misuse of employee software opportunities such as: Credit balances/accounts reconciliation, shipping/issuance/Inventories, TV: ACH initiation, authorization for cash and cash bank</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>LOW-RISK</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4.5</td>
<td>Fraudulent instruments</td>
<td>Creation of fictitious vendor/misrepresentation for personal gain</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>LOW-RISK</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4.6</td>
<td>Payroll theft</td>
<td>Fraudulent payment to employee, false deductions, false deductions</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>LOW-RISK</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5.1</td>
<td>Vendor abuse</td>
<td>Embezzlement, related party collusion, unexpected, fraudulent, professional liability, false reporting</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>LOW-RISK</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5.2</td>
<td>Related party transactions</td>
<td>Transactions are not at “Arm’s length”</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>LOW-RISK</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**SEC 210: Fraud Detection and Prevention**
### Fraud Risk Assessment

<table>
<thead>
<tr>
<th>Type of Fraud</th>
<th>Fraud Risk Number</th>
<th>Risk</th>
<th>Example of Threat</th>
<th>Potential Impact (High: 5, Medium: 3, Low: 1)</th>
<th>Factors Considered to Determine Potential Impact Rating</th>
<th>Probability of Fraud Occurrence (High: 5, Medium: 3, Low: 1)</th>
<th>Factors Considered to Determine Probability of Fraud Occurrence Rating</th>
<th>Combined Internal Risk Assessment Score</th>
<th>Overall Fraud Rating</th>
<th>Control(s) to Mitigate Internal Risk</th>
<th>Control Supporting Reference(s)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Corruption</td>
<td>5.3</td>
<td>Economic extortion</td>
<td>Self-serving use of misappropriation, laying in company's bank account</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>LOW RISK</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5.4</td>
<td>Conflict of Interest</td>
<td>Pressure results in services from an officer of the company's relative at a higher cost</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>LOW RISK</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2) Compliance</td>
<td>6.1</td>
<td>Bribery/Compromise</td>
<td>Under the table agent</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>LOW RISK</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>6.2</td>
<td>Occupational Safety Environment</td>
<td>Misidentification of data in transfer to concord deferred</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>LOW RISK</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>6.3</td>
<td>Regulatory</td>
<td>Changing data to comply with program requirements in order to gain incentives, compensation and/or advancement</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>LOW RISK</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>6.4</td>
<td>Malicious Discharge of Company Equipment</td>
<td>Deliberately destroy to frustrate investigation</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>LOW RISK</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SEC 210: Fraud Detection and Prevention
Fraud Risk Assessment

**DELIVERABLES - SIMPLIFIED HEAT MAP**

Fraud Risk Assessment Heat Map

R1-R18 are representative of risk factors identified in the Enterprise-wide Risk Assessment. Each Factor would be supported by a detailed description of the respective risk factor.
Figure 63: Primary Internal Control Weakness Observed by CFE

Source: ACFE Report to the Nations on Occupational Fraud and Abuse (2016)
Internal Controls

Designing and Implementing Controls

• Control Design
  ➢ Aligned with relevant fraud risks
  ➢ Executed by competent and objective individuals

• Control Effectiveness
  ➢ Evidence available to support whether control is operating as intended
  ➢ Control executed at a frequency appropriate to the fraud risk
Types of Controls

- **Preventive** – Intended to reduce the risk of fraud occurring to an acceptable level
- **Detective** – Intended to flag potential risk that a fraud occurred in a timely manner
- **Persuasive** – Tone and culture of the organization, its belief system
- **Competence** – Aptitude to recognize when something is not right
Internal Controls

Preventive Controls

• Human Resources procedures
  ➢ Recruiting/hiring – smart, honest, ethical
  ➢ Background investigations
  ➢ Anti-fraud training
  ➢ Exit interviews
• Restricted access (physical and system)
• **Segregation of duties** (limit keys to the kingdom)
• Authority limits
• Transaction-level controls – approvals, reviews
Internal Controls

Detection Controls

- Variance analysis – with communication and follow-up on unusual variances or items outside of thresholds
- Comparison of internal data to external sources
- Reconciliations
- Surprise audits
- Whistleblower hotline
- Exit interviews (HR)
Internal Controls

Detective Controls (Cont.)

• Independent reviews
• Physical inspections and counts
• Special audits (e.g., expense reports, P-card, cash counts)
Internal Controls

Persuasive Controls

- Formal code of ethics/conduct
- Whistleblower hotline
- Management setting appropriate example
- Positive workplace environment
- Honest and constructive feedback and recognition
  - Eliminate fear of delivering “bad news”
  - Treat employees with fairness
  - Organizational responsibilities clearly defined
  - Strong communication practices and methods
  - Direct communication vs. innuendo
Internal Controls

Competence

- Possesses required skill, knowledge, qualification, and/or capacity
- Requires knowledge of expected outcomes and incentives to report
- Is empowered to report concerns
- Effectively performs the duties of one's position
- Has an awareness of the duties of those around them
Internal Controls

Figure 47: Frequency of Anti-Fraud Controls

Source: ACFE Report to the Nations on Occupational Fraud and Abuse (2016)
DOJ Whistleblower Programs

False Claims Act (nicknamed the “Lincoln Law”)

- From 1986 to 2014, the United States government recovered $44 billion under the False Claims Act. More than two-thirds of this, about $30.3 billion, was recovered in cases filed by whistleblowers under the qui tam provisions of the False Claims Act.
- Whistleblowers have received over $4.7 billion under the False Claims Act. In 2014 alone, whistleblowers helped recover approximately $3 billion and were awarded over $435 million.
Resources

Ohio Auditor of State
https://ohioauditor.gov/fraud.html
1-866-Fraud-OH (1-866-372-8364)

U.S. Government Accountability Office (GAO)
1-800-424-5454

The Association of Government Accountants (AGA) - Fraud Prevention Toolkit
Https://www.agacgfm.org/Resources/Tools-To/Prevent-Fraud.aspx
Resources

Association of Certified Fraud Examiners (ACFE) - Report to the Nations on Occupational Fraud and Abuse – 2016 Global Study

AICPA Fraud Resource Center
http://www.aicpa.org/INTERESTAREAS/FORENSICANDVALUATION/RESOURCES/

The Institute of Internal Auditors
https://na.theiia.org/training/Pages/Fraud-Courses.aspx

Frank W. Abagnale
http://www.abagnale.com/company.htm
As one of the largest certified public accounting and business advisory firms in the region, Schneider Downs serves clients throughout the country and around the world. By integrating high-quality resources, systems and personnel, Schneider Downs has built a reputation of delivering individualized services built on insight, innovation, and experience to meet each client’s specific needs.

For more information, visit us at www.schneiderdowns.com

We Are Committed to Your Success

Schneider Downs