Developing a Fraud Risk Management Program

Erick O. Bell
Priyanka Jhang

Deloitte Financial Advisory Services LLP

September 11, 2013

Agenda

Making the case for a Fraud Risk Management Program

A COSO-consistent Process for Fraud Risk Management

Roles of Key Parties in Managing Fraud Risk

Control Environment and Fraud Risk Assessments

Anti-Fraud Control Activities

Sharing Information and Communication

Monitoring Activities

Making the case for a Fraud Risk Management Program

Fraud: Defined

Any illegal acts characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the application of threat of violence or of physical force. Frauds are perpetuated by individuals and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.

–Source: The Institute of Internal Auditors International Standards for the Professional Practice of Internal Auditing
–www.the.iia.org

Occupational Fraud: Defined

The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets.

—Source: 2006 Association of Certified Fraud Examiners Report to the Nation on Occupational Fraud & Abuse

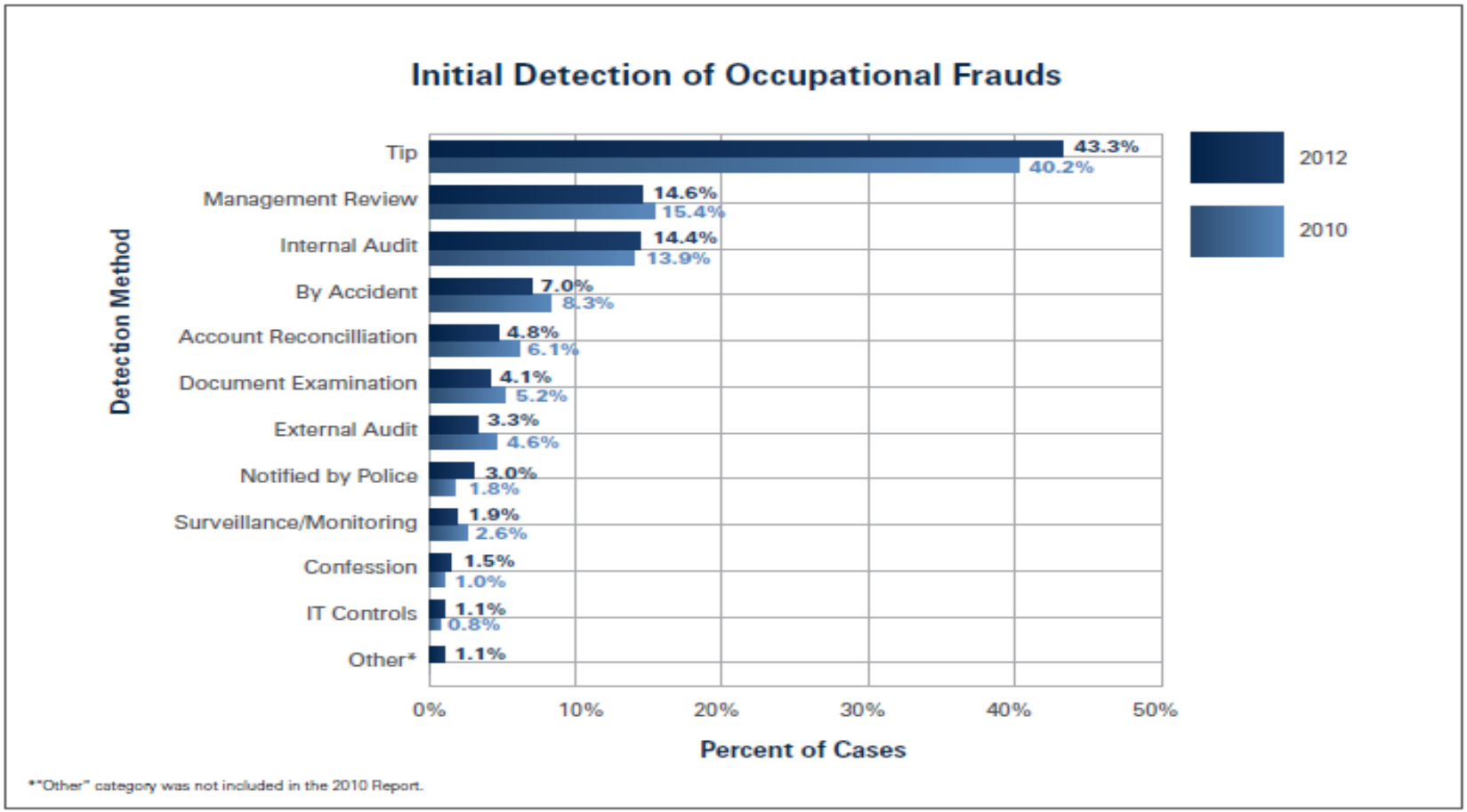
Errors Do Not Constitute Fraud

ACFE Fraud Statistics

- Losses = 5 percent of revenue
- $140,000 per case
- 18-month duration
- Highest impact to small businesses
- Higher positions = higher loss
- 81% of fraudsters displayed one or more red flags
  - Living beyond means
  - Financial difficulties
  - Unusually close association with vendors or customers
  - Excessive control issues

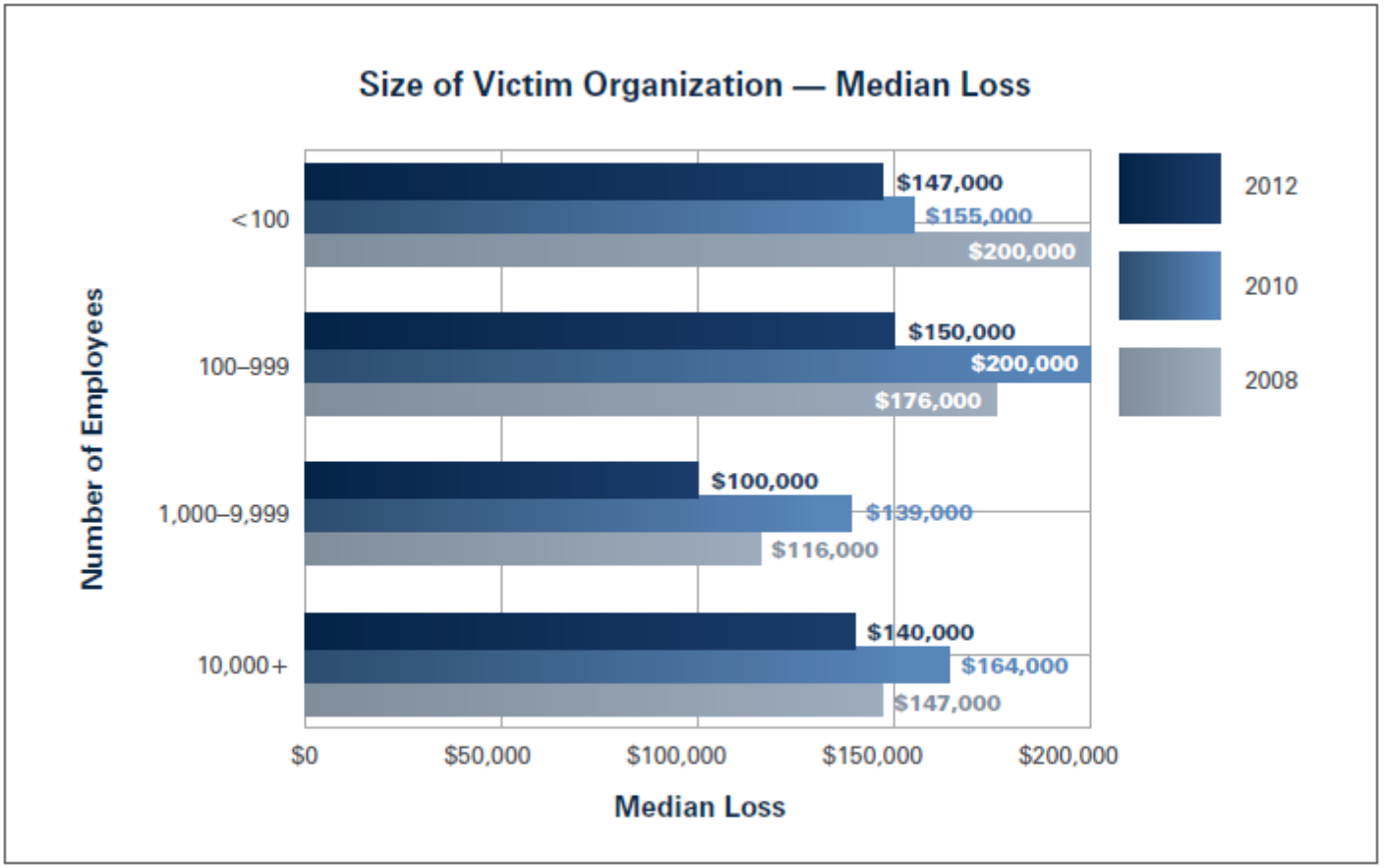
–Source: 2012 Association of Certified Fraud Examiners Report to the Nation on Occupational Fraud & Abuse

Detection of Fraud



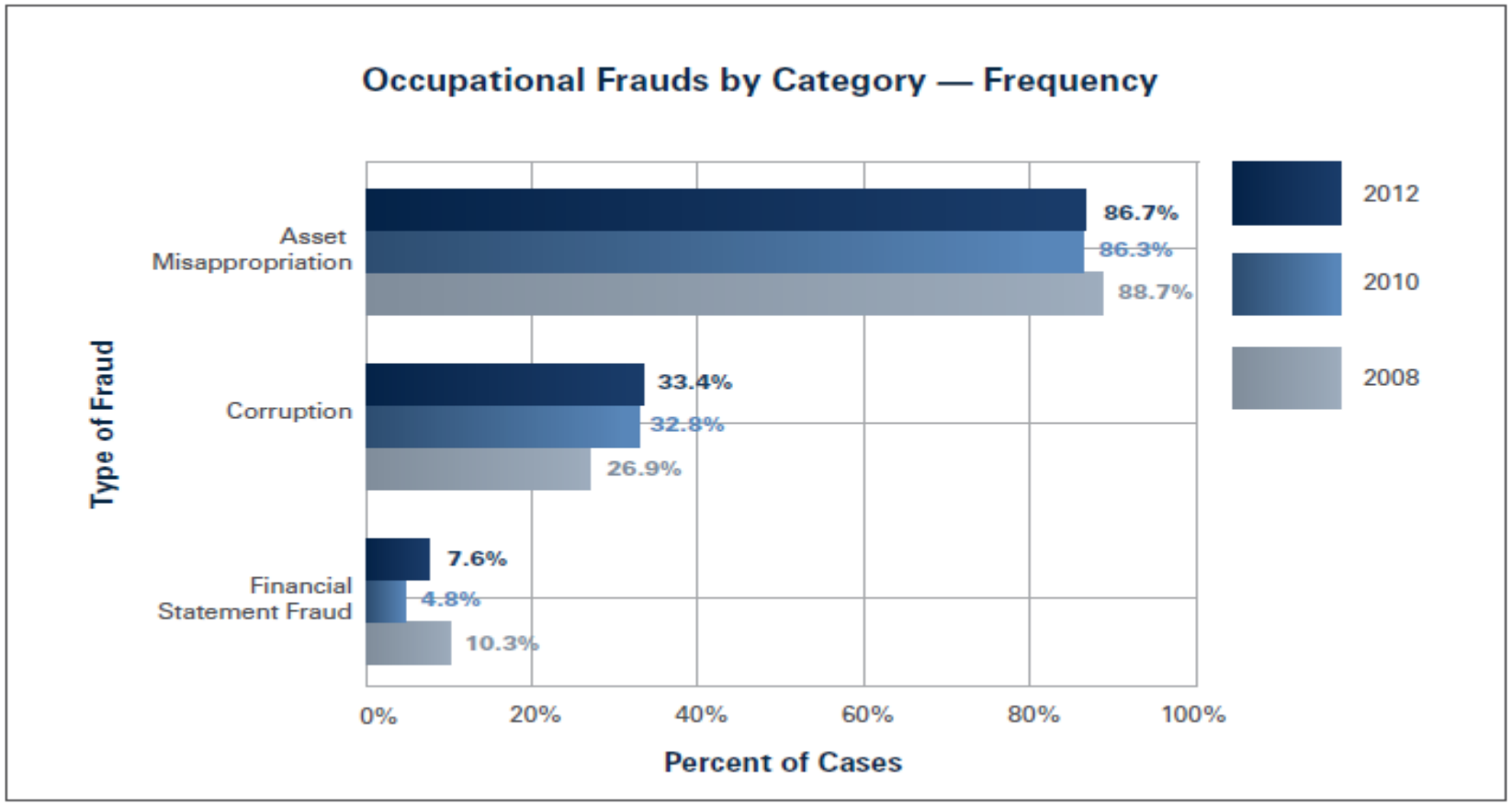
—Source: 2012 Association of Certified Fraud Examiners Report to the Nation on Occupational Fraud & Abuse

Size of Victim Organizations



—Source: 2012 Association of Certified Fraud Examiners Report to the Nation on Occupational Fraud & Abuse

Types of Occupational Fraud & Abuse



Percent of cases exceeds 100 percent due to cases spanning several categories.

—Source: 2012 Association of Certified Fraud Examiners Report to the Nation on Occupational Fraud & Abuse

Why Organizations Should Manage Fraud Risk

- Duty of care to shareholders/stakeholders
- Manage impact of fraud on profitability/available funding
- Statutory/regulatory requirements (Sarbanes-Oxley, SEC, FCPA, Federal Sentencing Guidelines, funding agency requirements)
- Employee morale
- Stakeholder confidence

Statutory and Regulatory Guidance/Requirements for Fraud Risk Management

- Sarbanes-Oxley Act
- IIA Practice Advisories
- SEC Enforcement Policies
- PCAOB Auditing Standards
- Foreign Corrupt Practices Act
- Office of Foreign Asset Control
- Federal Sentencing Guidelines Criteria
- Department of Justice Prosecution Policy
- AICPA — Management AFPC Guidance
- IIA/AICPA/ACFE — Managing the Business Risk of Fraud
- NYSE / NASDAQ — Corporate Governance Listing Standards
- AICPA — Management Override ("Achilles Heel")

Reasons Why Entities Need to Manage Fraud Risk

- Organizational Benefits
  - Survival
  - Greater Profitability
  - Intact or enhanced image
  - Improved efficiency & increased ability to meet commitments
  - Enhanced morale – attract/retain talent
- Individual Benefits
  - Morale
  - Reduced stress
  - Job satisfaction
  - Greater employment security

Questions

?

A COSO-consistent Process for Fraud Risk Management

COSO – An Overview

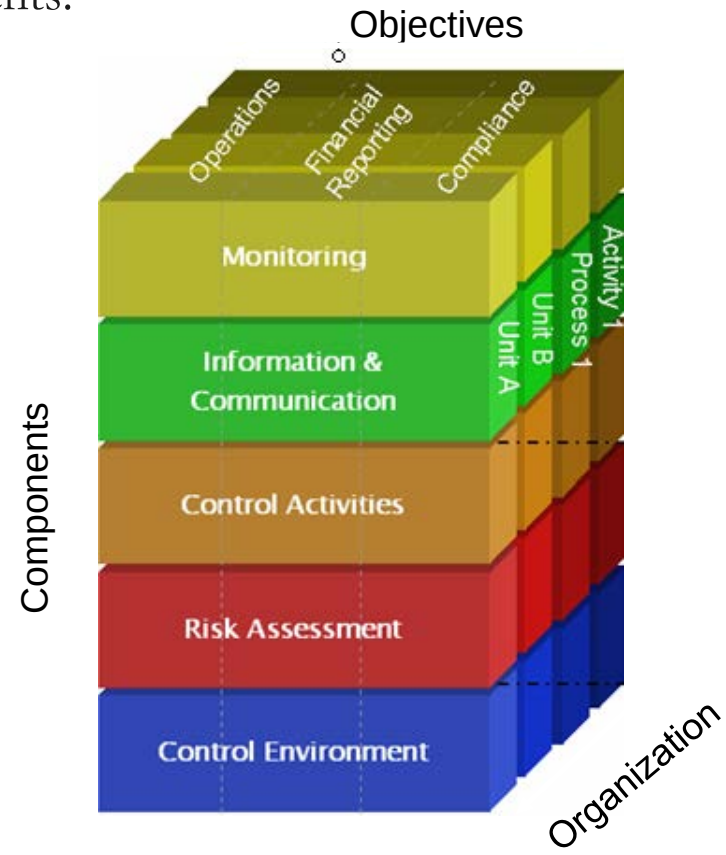
- The Committee of Sponsoring Organizations of the Treadway Commission ("COSO")
  - Formed specifically to study the causal factors that can lead to fraud
- Private sector initiative established in 1985 by the following organizations:
  - American Accounting Association ("AAA")
  - American Institute of Certified Public Accountants ("AICPA")
  - Financial Executives Institute ("FEI")
  - The Institute of Internal Auditors ("IIA")
  - Institute of Management Accountants ("IMA")

Internal Control – Integrated Framework (the "Framework")

- In 1992, COSO issued the Internal Control – Integrated Framework
  - Intended to help businesses and other entities assess and enhance their internal control systems
  - Underlying principles provide framework for proactively establishing an environment to manage fraud risk

The COSO Internal Control – Integrated Framework

- COSO offers an integrated framework that defines internal control by five interrelated components:
  - Control Environment
  - Risk Assessment
  - Control Activities
  - Information & Communication
  - Monitoring
- The COSO framework helps clarify the context of internal control discussions



Recognized as an Internal Control Standard

- Organizations are continually being held to increased standards for internal control
  - Sarbanes Oxley Act of 2002
  - PCAOB Auditing Standard No. 5
  - Federal Sentencing Guidelines
- COSO Framework is well known and recognized as authoritative
  - The COSO Framework has served as the internal control standard for organizations implementing and evaluating internal control in compliance with the US Sarbanes-Oxley Act of 2002 ("SOX") and the US Public Company Accounting Oversight Board ("PCAOB") Standard[s] 2 [and 5] [1]
  - Recognized by executives, board members, regulators, standard setters, professional organizations, and others as an appropriate comprehensive framework for internal control

[1] New Guidance for Small Businesses to be Released, July 7, 2006, Institute of Internal Auditors

It's all changing.....

Not really.....

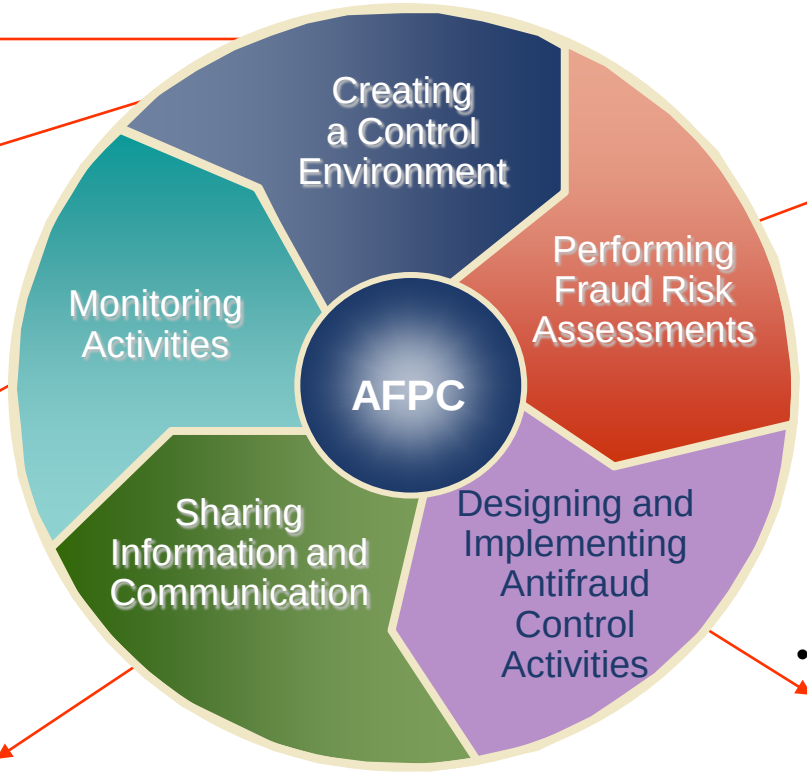
The New Internal Control –Integrated Framework

- Old framework will be superseded in December 2014
- Same 5 components
- 17 principles
  - "8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.

A COSO-Consistent Approach

- Tone at the top
- Code of Conduct/Ethics
- Whistleblower Hotline

ICFR



- Identify fraud risk factors, fraud risks and fraud schemes
- Monitoring effectiveness of antifraud programs and controls
- Effective communication of antifraud programs and controls
- Link or map identified fraud risks to control activities

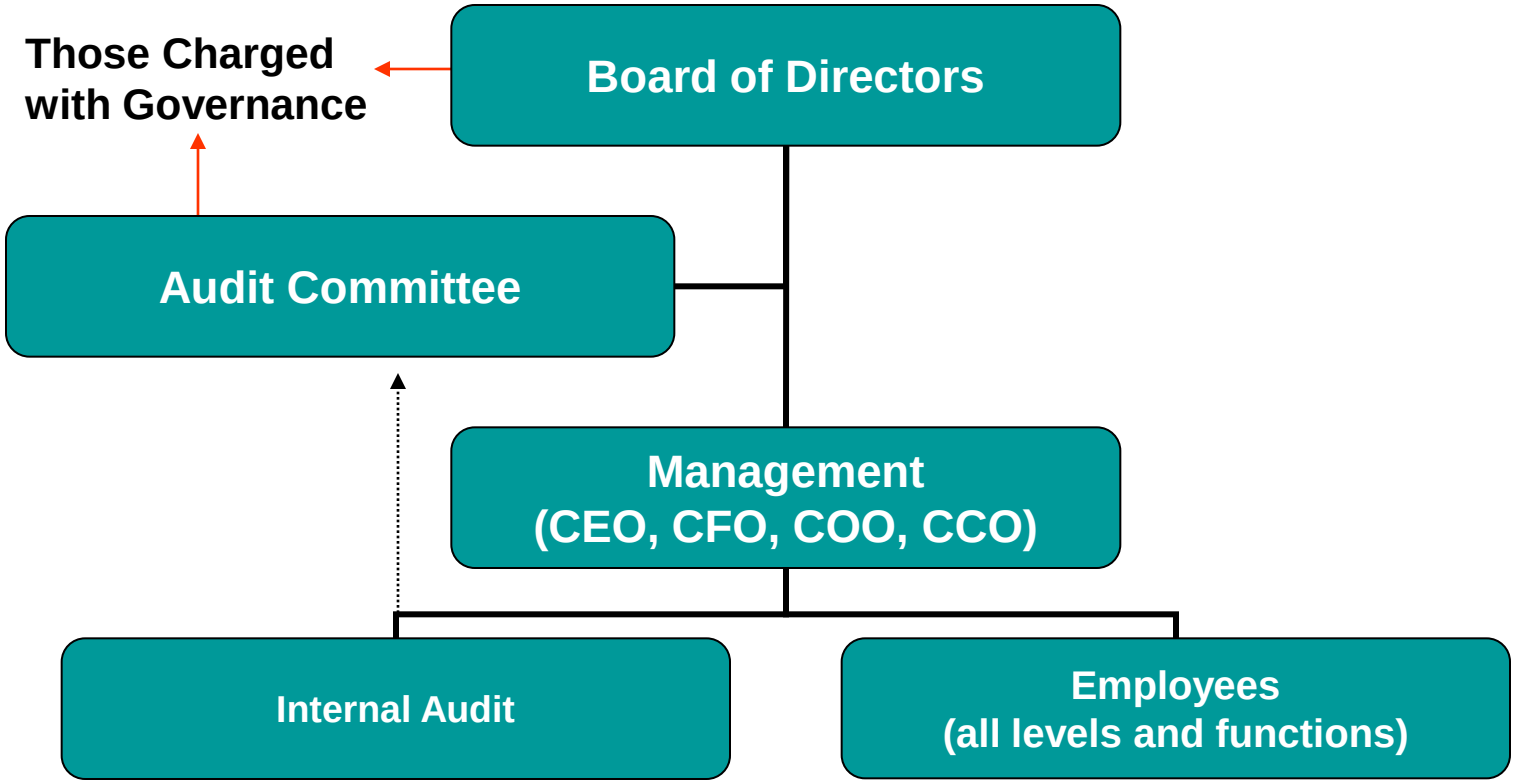
5 Elements Source: Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control – Integrated Framework*

Questions

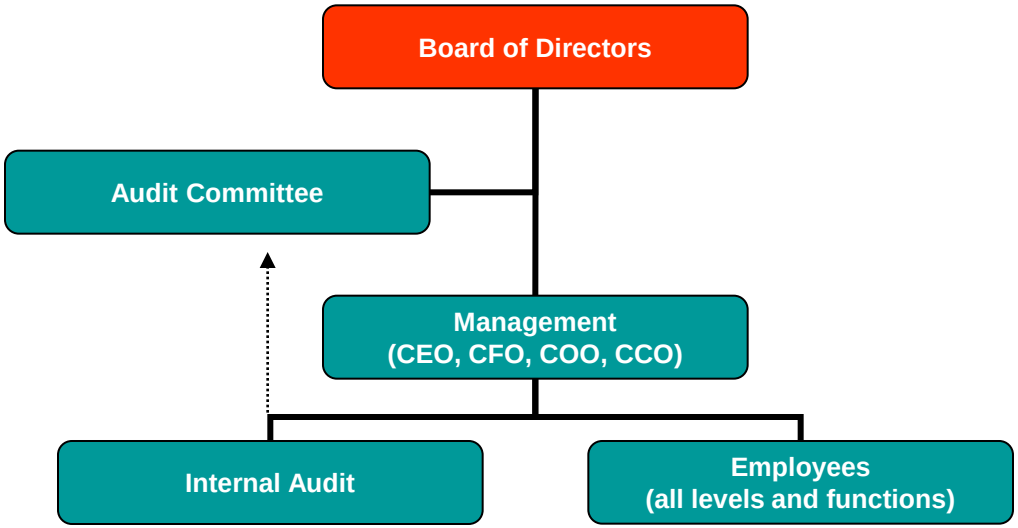
?

Roles of Key Parties in Managing Fraud Risk

3: Key Parties Involved with Managing Fraud Risk

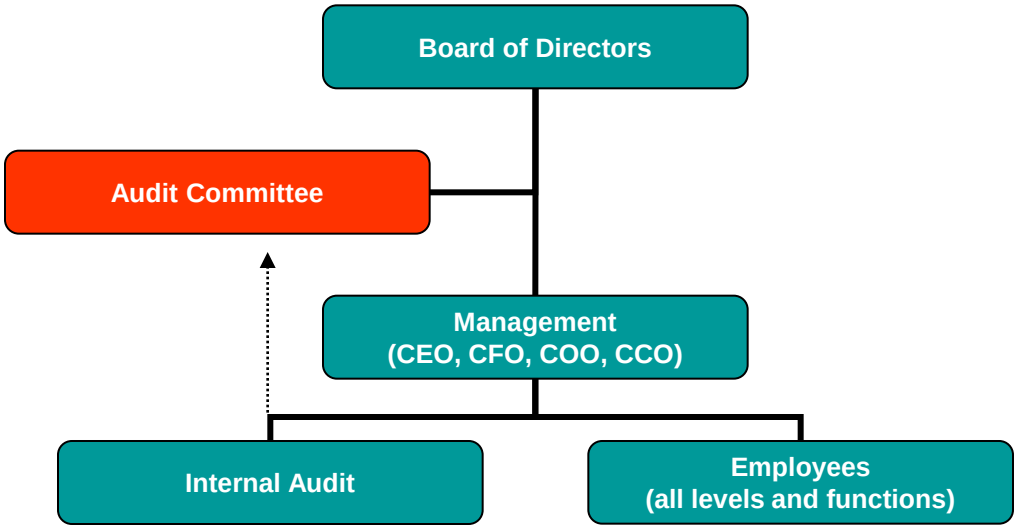


Roles & Responsibilities – Board of Directors



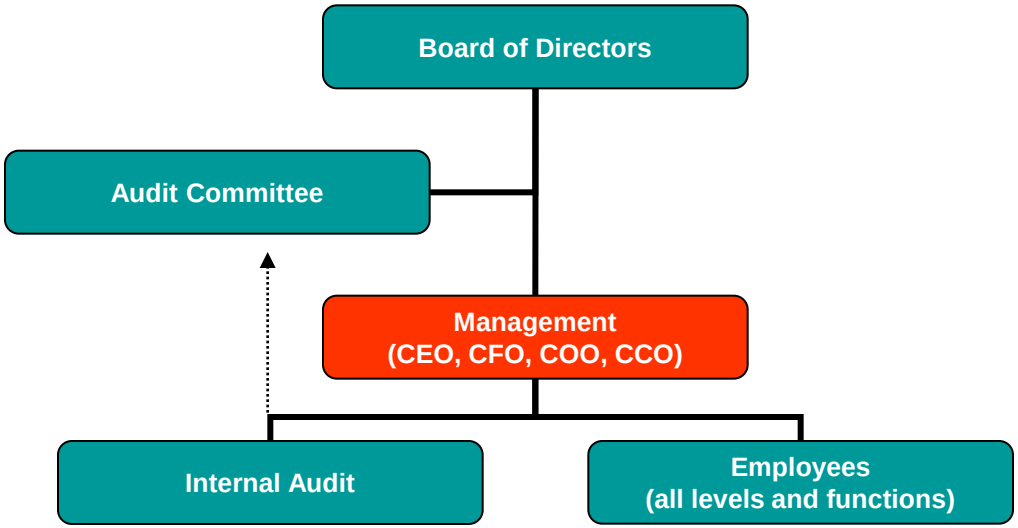
- Ensure that management designs effective fraud risk management documentation to encourage ethical behavior
- Understand fraud risks (both generally and those affecting the organization)
- Establish and communicate an appropriate level of risk tolerance for the organization
- Maintain oversight of the fraud risk assessment
- Monitor management's reports on fraud risks, policies, and control activities
- Ability to retain outside experts where needed
- Assure that external auditors understand the Board's active involvement in fraud risk management

Roles & Responsibilities – Audit Committee



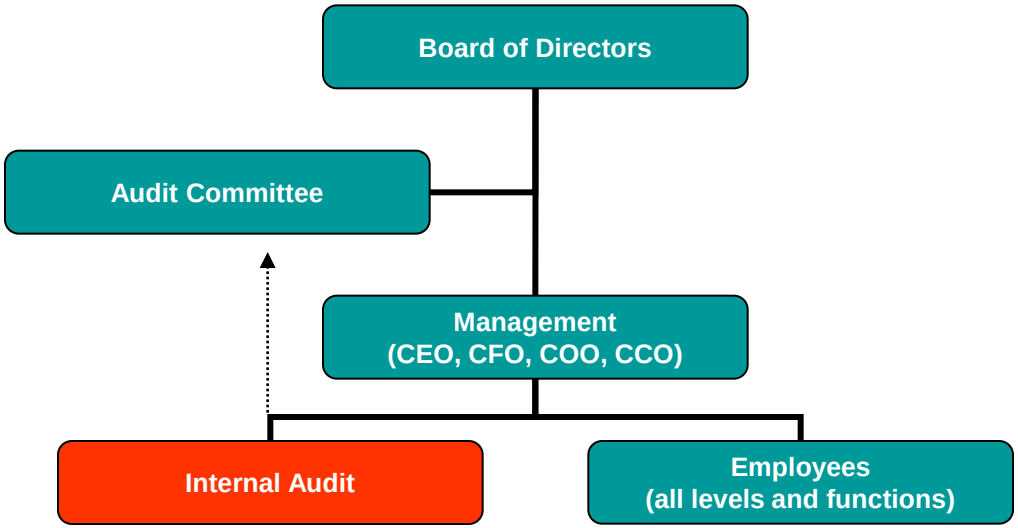
- Active role in the oversight of the fraud risk assessment
- Addressing the risk of management override of controls
- Uses internal audit, or other designated personnel, to monitor fraud risks throughout the organization
- Meet separately with appropriate individuals (e.g., internal audit, external auditors)
- Maintain awareness of the external auditor's responsibilities pertaining to fraud
- Seek advice of counsel when dealing with allegations of fraud
- Provide specific consideration to reputation risk when reviewing work of management, internal audit, external auditors

Roles & Responsibilities – Management



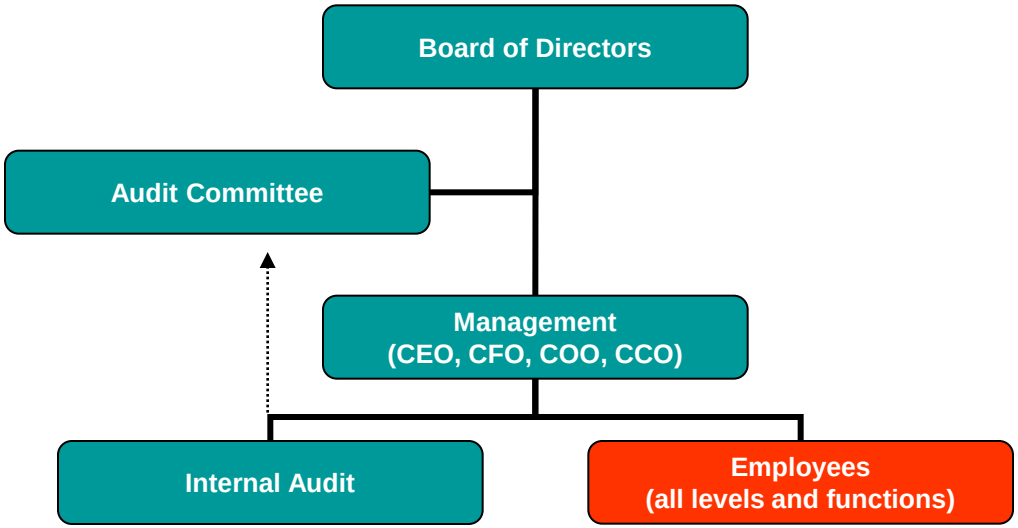
- Design and implementation of a fraud risk management program
- Implementing and documenting a fraud risk assessment process
- Maintaining adequate documentation of design of antifraud programs and controls
- Evaluating design and operating effectiveness of antifraud programs and controls
- Reporting to the Board on actions that have been taken to manage fraud risks and the effectiveness of the fraud risk management program
- Educating the organization on areas of potential compliance violations
- Enforcing Code of Ethics

Roles & Responsibilities – Internal Audit



- Provide assurance to the Board and to management that existing controls are appropriate given the risk tolerance established by the Board
- Review the comprehensiveness and adequacy of the risks identified by management, especially regarding management override risks
- Support management's education of the organization regarding areas of potential fraud and compliance violations
- Consider fraud risks when developing annual audit plan and spend time to evaluate the design and operation of antifraud controls
- Support the audit committee in performing detective activities around the risk of management override of controls

Roles & Responsibilities – Employees



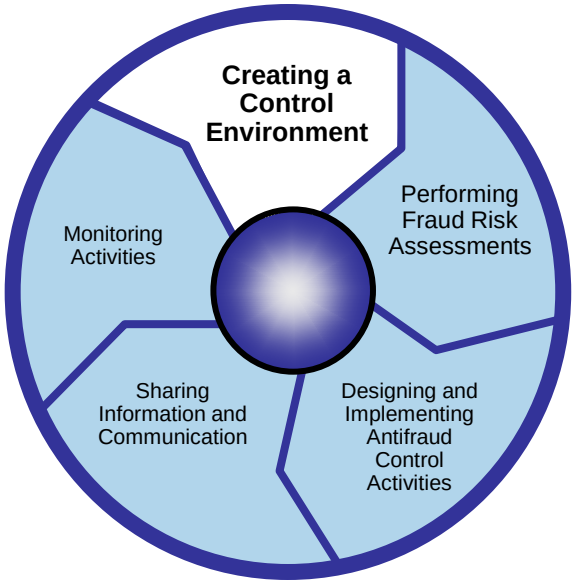
- Basic understanding of fraud and awareness of red flags
- Understand their roles within the internal control framework, specifically how their procedures are designed to manage fraud risk
- Read and understand policies and procedures (e.g., fraud policy, code of conduct, whistleblower policy)
- Participating in the process of creating a strong control environment
- Report suspicions or incidences of fraud and corruption
- Cooperate with investigations

Questions

?

Control Environment and Fraud Risk Assessments

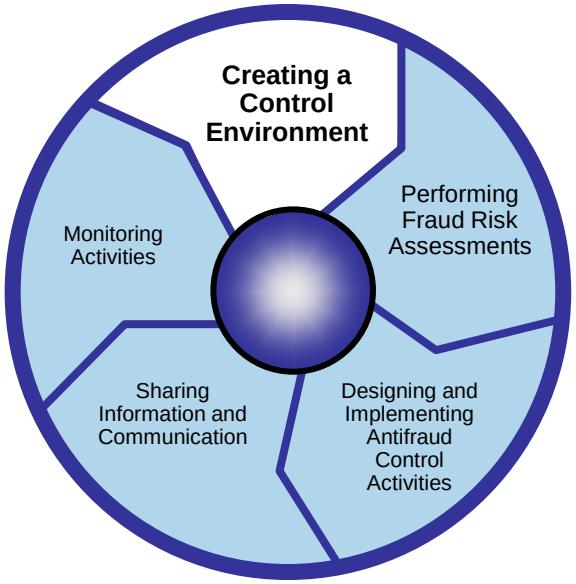
COSO Overview: Control Environment



Control Environment

- Control consciousness of an organization; it is the environment in which people conduct business activities and fulfill their control obligations.
- The control environment includes both intangible and tangible elements:
  - Integrity and ethical values
    - Incentives
    - Communicating moral values
  - Commitment to competence
  - Governance and organization structure
  - Management's philosophy and operating style
  - Assignment of authority and responsibility
  - Human resource policies and practices

COSO Overview: Control Environment



- Some of the components of the control environment in which management may focus its efforts include:
  - Audit Committee
  - Management Accountability
  - Fraud control policy/strategy
  - Tone at the Top
  - Code of Conduct and Ethics
  - Hiring and Promotion Procedures
  - Hotlines/helplines
  - Investigation and corrective action

What is a Fraud Risk Assessment?

- Fraud risk assessment is an integral part of an antifraud program that is based on the COSO framework
- A crucial part of an entity's broader risk assessment process, a fraud risk assessment considers the ways that fraud and misconduct can occur by and against the entity

Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control – Integrated Framework*

Benefits of A Fraud Risk Assessment

- Help in meeting **regulatory** requirements
- Assist in providing structure to tackling the potential of fraud in a **proactive** manner
- **Reduce exposure from fraud risk**, with potential impact on bottom line
- Supplement the internal controls environment in helping to **prevent, detect and deter fraud**
- Help address areas of exposure in an organization where the internal controls environment may have **limitations, such as collusion**

Management's Fraud Risk Assessment Overview

	Step	Approach	Output
1	Identify & Evaluate Fraud Risk Factors	▪ Identify fraud risk factors	▪ Schedule of fraud risk factors ▪ Sound knowledge of fraud risk environment
2	Identify Possible Fraud Schemes & Scenarios	▪ Identify fraud risks ▪ Identify specific fraud schemes ▪ Identify account balances and potential errors related to each fraud risk	▪ Pervasive & specific fraud risks ▪ Catalog of fraud schemes
3	Analyze Fraud Risks & Evaluate Control Design & Implementation	▪ Analyze the likelihood and significance of possible fraud schemes ▪ Link fraud schemes to mitigating controls & evaluate control design and implementation	▪ Inherent Risk Rating (IRR) of entity ▪ Catalog of existing controls ▪ Fraud Control Risk Rating ▪ Fraud Risk Related Control Gap Analysis
4	Evaluate Fraud Risk Assessment Results & Prioritize Residual Fraud Risks	▪ Evaluate the results of fraud risk analysis against established criteria and prioritize risks for treatment	▪ Residual Risk Rating (RRR) ▪ Identification of fraud risks requiring further treatment ▪ Fraud risks prioritized
5	Risk Treatment	▪ Prepare Fraud Risk Action Plan ▪ Implement Plan	▪ Fraud Risk Action Plan ▪ Fraud Risks Treated

Where do Fraud Risk Assessments Typically Fall Down?

- Appropriate personnel are not involved in the process
- Assessment consists of an identification of risk factors only, and does not include an identification of schemes & scenarios
- Potential perpetrators are not identified (which can lead to insufficient consideration of management override)
- Does not consider collusive fraud and management override of controls
- Lack of monitoring by the Audit Committee/Board
- Lack of follow up after identification of fraud risks and linkage to mitigating controls

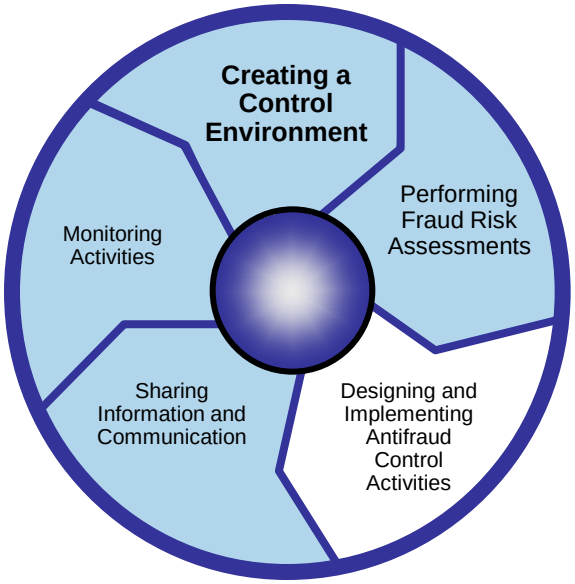
Questions

?

Anti-Fraud Control Activities

Design and Implement Control Activities

- Management may focus on several considerations when designing and implementing antifraud control activities, including:
  - Preventive Controls
  - Detective Controls
- Management may identify preventive controls, detective controls, or a combination of both, as adequately addressing financial reporting risks. (SEC ICFR guidance)



Antifraud Control Activities – Prevent, Detect, & Deter

Preventive Controls	Detective Controls
• Designed to mitigate the opportunity for an individual to perpetrate a fraud • Limited effectiveness when management may be involved in the fraud • Serve as a deterrent by creating an additional obstacle to carrying out a fraud	• Designed to identify indicators of a fraud, if committed • May be used as a monitoring activity to assess effectiveness of other antifraud controls • Serves as a deterrent by heightening the perceived likelihood of being caught

Source: Managing the Business Risk of Fraud: A Practical Guide

Antifraud Objectives for Control Activities: Mitigate

- Control activities designed to mitigate fraud are not always the same as the organization's internal control activities designed to identify errors.
- Antifraud control activities represent actions taken by management to mitigate the specific fraud risks identified in the risk assessment process.
  - These are more specialized in both their design and application.

Source: Managing the Business Risk of Fraud: A Practical Guide

Risk-Based Approach

- Begins with the fraud risk assessment
- Design control activities to address most likely & significant inherent and residual fraud risk
  - Overall risk tolerance - established by the board of directors or similar governance
  - Board should ensure management has implemented the proper level of controls based upon established risk tolerance level
  - Controls identified as antifraud controls should be evaluated for operating effectiveness and executed by competent and objective individuals

Effective Fraud Controls

- Fraud risk management often uses two types of controls:
  - Entity-level controls, such as:
    - Tone at the top
    - Code of conduct and ethics
    - Hiring and promotion procedures
    - Whistleblower hotline
  - Process-level controls, such as:
    - Disbursement approvals
    - Journal entry approvals
    - Management or supervisor reviews
    - Computer system access controls

Fraud Prevention

- Awareness is key to prevention
  - Policies – Corporate governance
  - Procedures – Design of antifraud programs and controls
  - Training, Communication, and Affirmation
- Human Resources may also play an integral role in fraud prevention
  - Conducting background investigations
  - Hiring the competent people
  - Evaluating performance and compensation programs
  - Conducting exit interviews
- Aligning individual responsibilities with the level of one's authority
- Transaction level procedures (e.g., reviews, financial reporting and internal control competencies)
- Continuous monitoring

Characteristics of Fraud Detection

- Occurs in the ordinary course of business
- Draws on external information to corroborate internally generated information
- Formally and automatically communicates identified deficiencies and exceptions to appropriate organizational leadership
- Uses results to enhance and modify other controls

Fraud Detection

- Three primary ways fraud is detected:
  - Anonymous Reporting (Hotline Tip)
    - Most likely means of detecting fraud
    - Employees should not fear retaliation
  - Process Related Controls
    - Reconciliations/Authorization levels
    - Physical counts/Inspections
    - Segregation of duties
  - Internal Auditing

* Appearance of strong detection controls in place can provide most significant deterrent to fraud.

Proactive Fraud Detection

- Detective control activities are based on risk assessment and fraud attributes
- Detect anomalies, trends, risk indicators
- Continuous auditing (monitoring)
- Data analytics

* Appearance of strong detection controls in place can provide most significant deterrent to fraud.

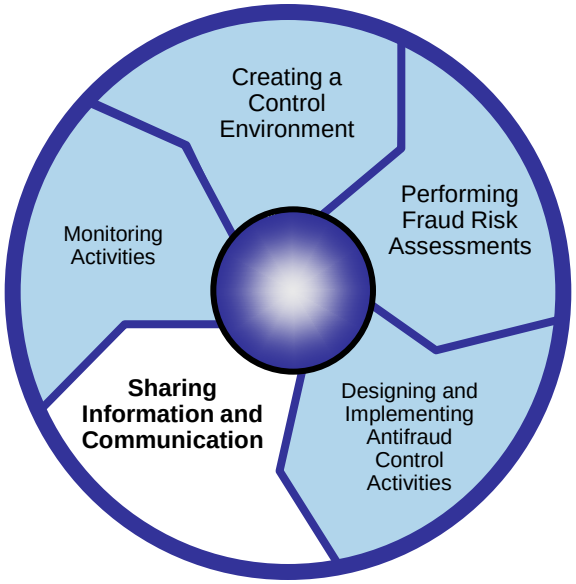
Questions

?

Sharing Information and Communication

Sharing Information and Communication

- The **manner** and **frequency** with which management communicates the purpose and existence of its fraud controls can greatly impact the effectiveness of those controls



Sharing Information and Communication: Objective

- As it relates to fraud risk management, what are some key **objectives** of sharing information and communication?
- Objectives of sharing information and communication:
  - Convey a clear message about the corporate culture
  - Set expectations about ethical employee behavior
  - Remind employees about their roles and responsibilities for maintaining an ethical work environment
  - Maintain awareness of reporting mechanisms available to employees
  - Reinforce the ramifications of improper or unacceptable behavior in order to deter others from similar actions

Sharing Information and Communication: Tone at the Top

- Management has a responsibility to clearly **communicate the tone at the top**
- Communication of the tone at the top includes sharing management's expectations for ethical behavior by all employees
- Mechanisms include:
  - Setting an example ("Walking the Talk")
  - Code of conduct
  - Intranet site providing information on ethics and AFPC
  - Broadcast emails and/or voicemails
  - Corporate newsletters addressing ethics and AFPC
  - CEO speeches or message on the importance of ethics and integrity

Sharing Information and Communication: Information Flow

- **Effective communication must flow top down and bottom up**
- There should be:
  - Open channels of communication
  - A clear-cut willingness to listen
- Mechanisms include:
  - Normal reporting channel
  - Separate lines of communication (e.g., a channel directly to a senior officer, chief internal auditor, or legal counsel)
  - Whistle-blower hotline/ombuds office/ethics office/compliance office
  - Broadcast emails/voicemails
  - Organization wide meetings, newsletters, web cast
  - Intranet site

Sharing Information and Communication: External Parties

- **An organization should maintain open channels of communication with customers, suppliers, and other external parties**
- Mechanisms include:
  - Providing customers, suppliers, and other external parties with copies of your ethics guidelines
  - Providing outside parties with a whistle-blower phone number or email address to facilitate feedback
  - Surveying outside parties (customers, vendors) on their perception of the integrity and ethical values of company personnel by company personnel independent of the main customer/vendor contact
  - Meeting with the external auditor or regulator upon the completion of their examination to discuss findings and propose resolutions
  - Collaboration between internal audit departments of major customers and vendors

Sharing Information and Communication: Training

- Management may assess whether its training programs include:
  - Training for new employees about matters of fraud and the entity's code of conduct and ethics
  - Periodic training for existing employees addressing changes in the business environment
  - Training that is tailored to the roles and responsibilities of employees
  - Education about when and how to utilize the whistle-blower system; encourage proper reporting

Sample Email – Ethics awareness

- **Sometimes, it either is, or it isn't.**
- You either sank the putt, or you didn't. No two ways about it. And in business, some ethics issues are just like that. What's right or wrong is clear, obvious, and unarguable. But other times, it's far less clear. So stay alert. Pay attention to shades of gray. Tune in to your intuition
- If you feel something's not quite right in an ethical sense, call a halt to play. Consult with peers and colleagues you respect. Research the rules
- And remember, the Integrity Helpline is always there. You can ask a question or file a report, via the **Web** or phone (888-XXX-XXXX), 24-hours-a-day, every day of the year, from anywhere in the world
- These days, ethics has to be a hole in one. Every time.
- For further information about Ethics and Compliance, go to the Company's intranet site (provide link)

Sample Email – Ethics awareness

- **Sometimes, it's pretty hard to be uncertain.**
- You have the winning hand, or you don't. It's very clear to everyone. In business, some ethics issues can be just like that. Clear, obvious, and unarguable
- But other times, it's far less apparent. So stay alert. Pay attention to shades of gray. Listen to your intuition
- And if something feels wrong, don't play your cards too close to your vest. Stop play. Revisit the rules. Consult with peers and colleagues whose opinions you respect
- If you have questions, the Integrity Helpline is always there. You can ask a question or file a report, via the Web or phone (+1 888 XXX XXXX), 24-hours-a-day, every day of the year, from anywhere in the world
- Today, the winning hand in business is doing what's ethically right—for our colleagues, our professions and our clients.
- For further information about Ethics and Compliance, go to the Company's intranet site (provide link)

Delivering Training Cost Effectively

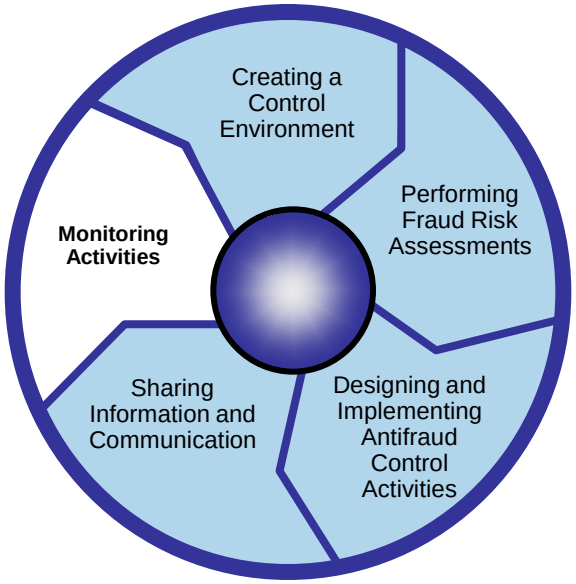
- What are best practices for delivering training cost effectively?
  - Consider the audience
  - Consider the mode:
    - Lecture
    - Text
    - Simulation
  - Consider the medium:
    - In person
    - Paper based
    - Electronic\Web Based
  - Consider the:
    - Timing
    - Duration
    - Frequency

Questions

?

Monitoring Activities

COSO Overview: Monitoring

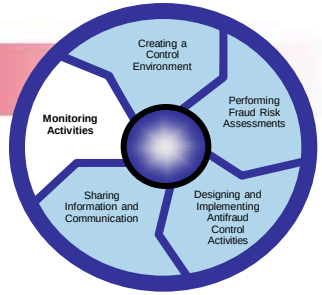


Monitoring Activities

- Ongoing periodic monitoring of AFPCs are vital to management's ability to react to the changing business environment and related impact on fraud risks.

Monitoring activities support:	Management	Ensures that controls are operating effectively
	Those charged with governance	Provides assurance that management is executing its internal control responsibilities effectively

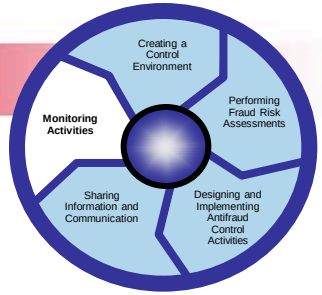
Monitoring: Two Fundamental Components



Assess operating effectiveness	• Monitoring should be designed to assess the operating effectiveness of internal control components • Internal control performance should be assessed over time through ongoing monitoring of operations and separate periodic evaluations • Scope and frequency of monitoring activities depend on significance of risks being controlled and the importance of controls in reducing risks • Monitoring activities should be built into normal, recurring operating activities of an organization • Monitoring activities may include [1]: – Controls to monitor results of operations – Controls to monitor other controls, including activities of the internal audit function, the audit committee, and self-assessment programs
Identify and report deficiencies	• Deficiencies in internal control should be identified and communicated in a timely fashion to those parties responsible for taking corrective action • Organizations should have: – A defined escalation path for reporting and follow-up – Accountability for corrective action to address the root cause of the control weakness

[1] SEC 404 Guidance, Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities and Exchange Act of 1934

Examples of Monitoring Activities



Periodic Evaluations	• Frequent and timely account reconciliations • Compliance testing by internal audit • Confirmation of information with external parties • Periodic confirmation from employees (code of conduct compliance) • Anomaly detection programs • Review of operating units' financial reports by higher levels of management
Continuous Monitoring	• Anomaly detection using software (e.g., ACL) • Journal entry testing

Using technology for effective monitoring

- Automated controls can play a significant role in enhancing the effectiveness, efficiency, and timeliness of monitoring [1]
- Monitoring tools typically focus on one or more of the following:
  - Transaction data
  - Conditions
  - Changes
  - Processing integrity
  - Error management

[1] COSO Guidance on Monitoring Internal Control Systems, September 2007, Discussion Document, Pages 23-24

Contact Information

Erick O. Bell
erbell@deloitte.com
(415) 783 6694

Priyanka Jhang
pjhang@deloitte.com
(213) 593 3753

DISCLAIMER

These materials and the information contained herein are provided by Deloitte Financial Advisory Services LLP ("Deloitte FAS") and are intended to provide general information on a particular subject or subjects and are not an exhaustive treatment of such subject(s).

Accordingly, the information in these materials is not intended to constitute accounting, tax, legal, investment, consulting, or other professional advice or services. The information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

These materials and the information contained therein are provided as is, and Deloitte FAS makes no express or implied representations or warranties regarding these materials or the information contained therein. Without limiting the foregoing, Deloitte FAS does not warrant that the materials or information contained therein will be error-free or will meet any particular criteria of performance or quality. Deloitte FAS expressly disclaims all implied warranties, including, without limitation, warranties of merchantability, title, fitness for a particular purpose, non-infringement, compatibility, security, and accuracy.

Your use of these materials and information contained therein is at your own risk, and you assume full responsibility and risk of loss resulting from the use thereof. Deloitte FAS will not be liable for any special, indirect, incidental, consequential, or punitive damages or any other damages whatsoever, whether in an action of contract, statute, tort (including, without limitation, negligence), or otherwise, relating to the use of these materials or the information contained therein.

If any of the foregoing is not fully enforceable for any reason, the remainder shall nonetheless continue to apply.