

**Council of Senior Business  
Administrators  
SOX Workshop**

***Internal Controls/Fraud***

**Presented by: Charley B. Clark  
February 1, 2006**

# Internal Control

**Definition:** A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

# Internal Control

## Key Concepts:

- Internal control is a *process*. It's a mean to an end, not an end in itself.
- Internal control is effected by *people*. It's not merely policy manuals and forms, but people at every level of an organization.
- Internal control can be expected to provide only *reasonable assurance*, not absolute assurance, to an entity's management and board.
- Internal control is geared to the achievement of *objectives* in one or more separate but overlapping categories.

# COSO

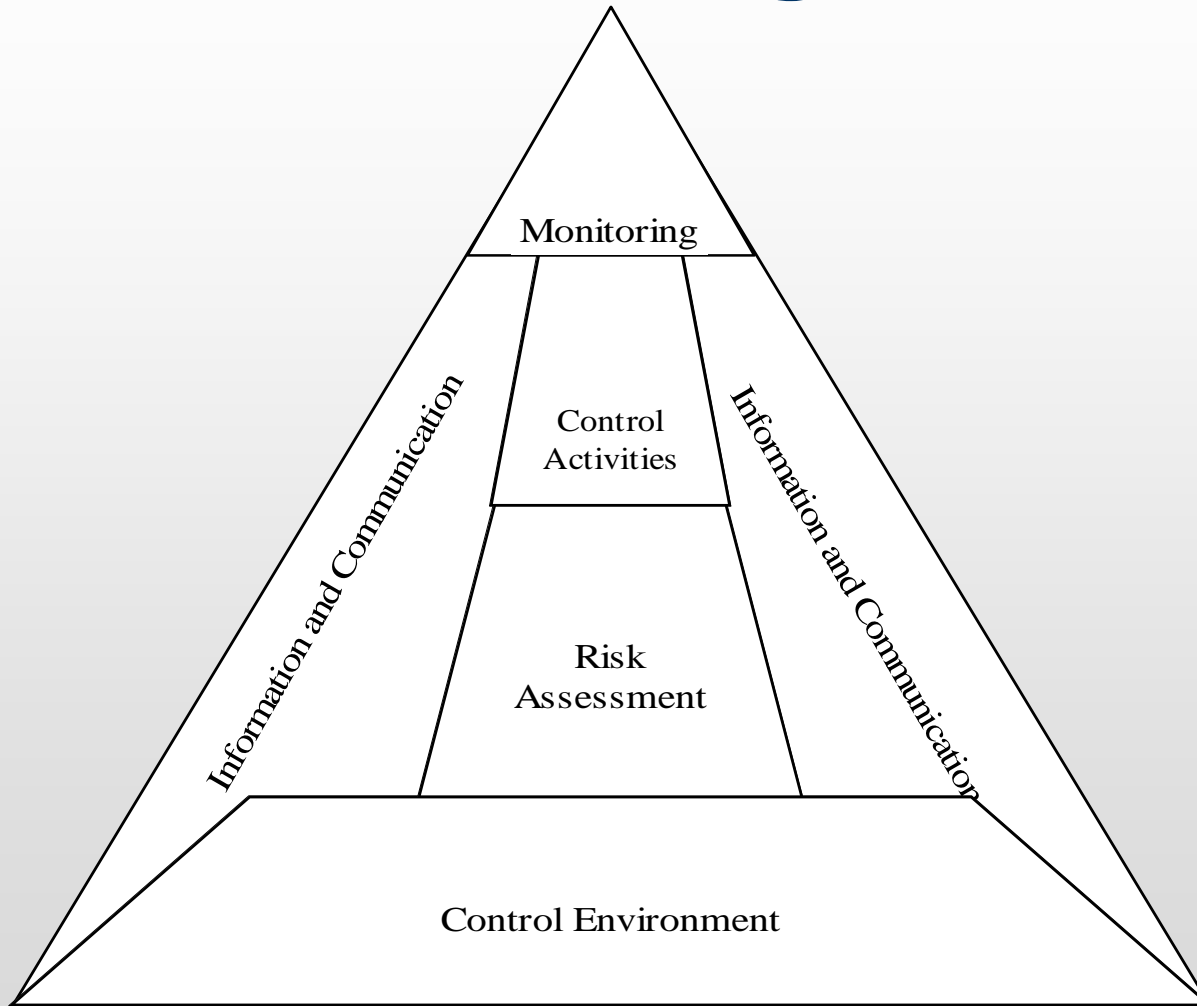
- Committee of Sponsoring Organizations of the Treadway Commission (COSO) created a model
  - Links internal control and organizational objectives
  - Covers all aspects of business operations

# COSO Model

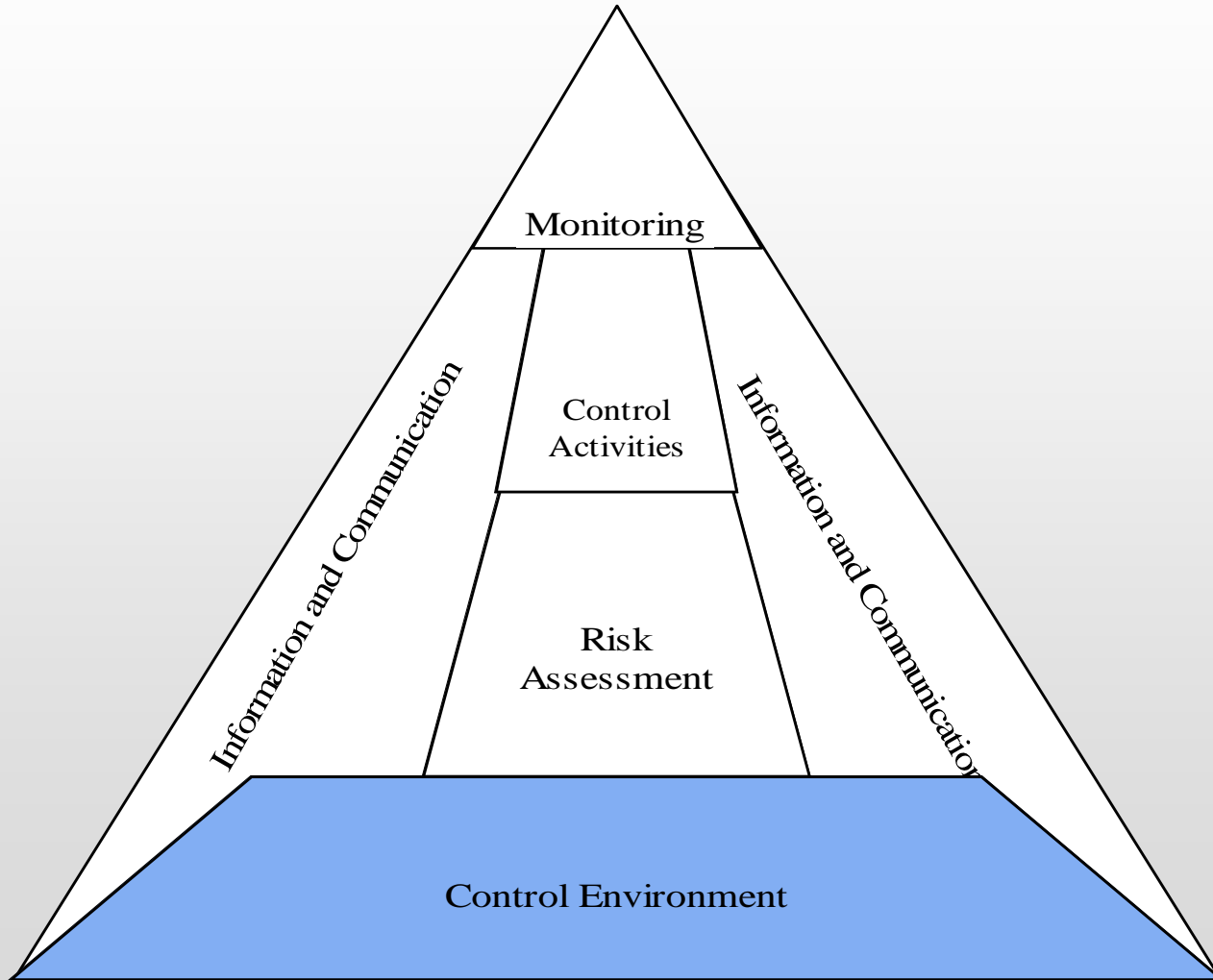
## **Five Components:**

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring

# COSO Diagram



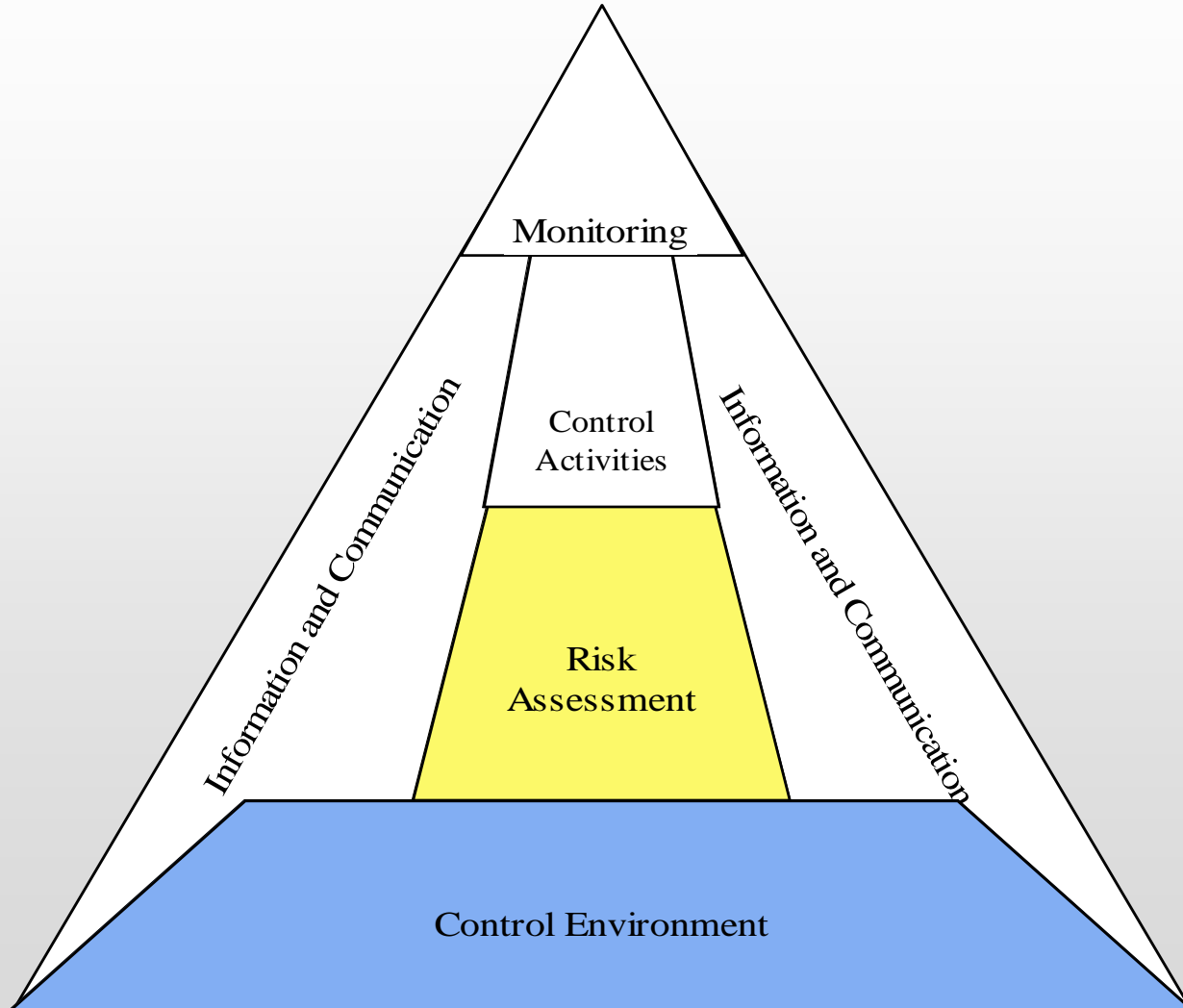
# COSO Diagram



# Control Environment

- Sets tone for organization and serves as a foundation for the other components
  - Integrity and ethical values
  - Commitment to competence
  - Board of Regents' oversight
  - Management's philosophy and operating style
  - Organizational structure
  - Assignment of authority and responsibility
  - Human Resources policies and procedures

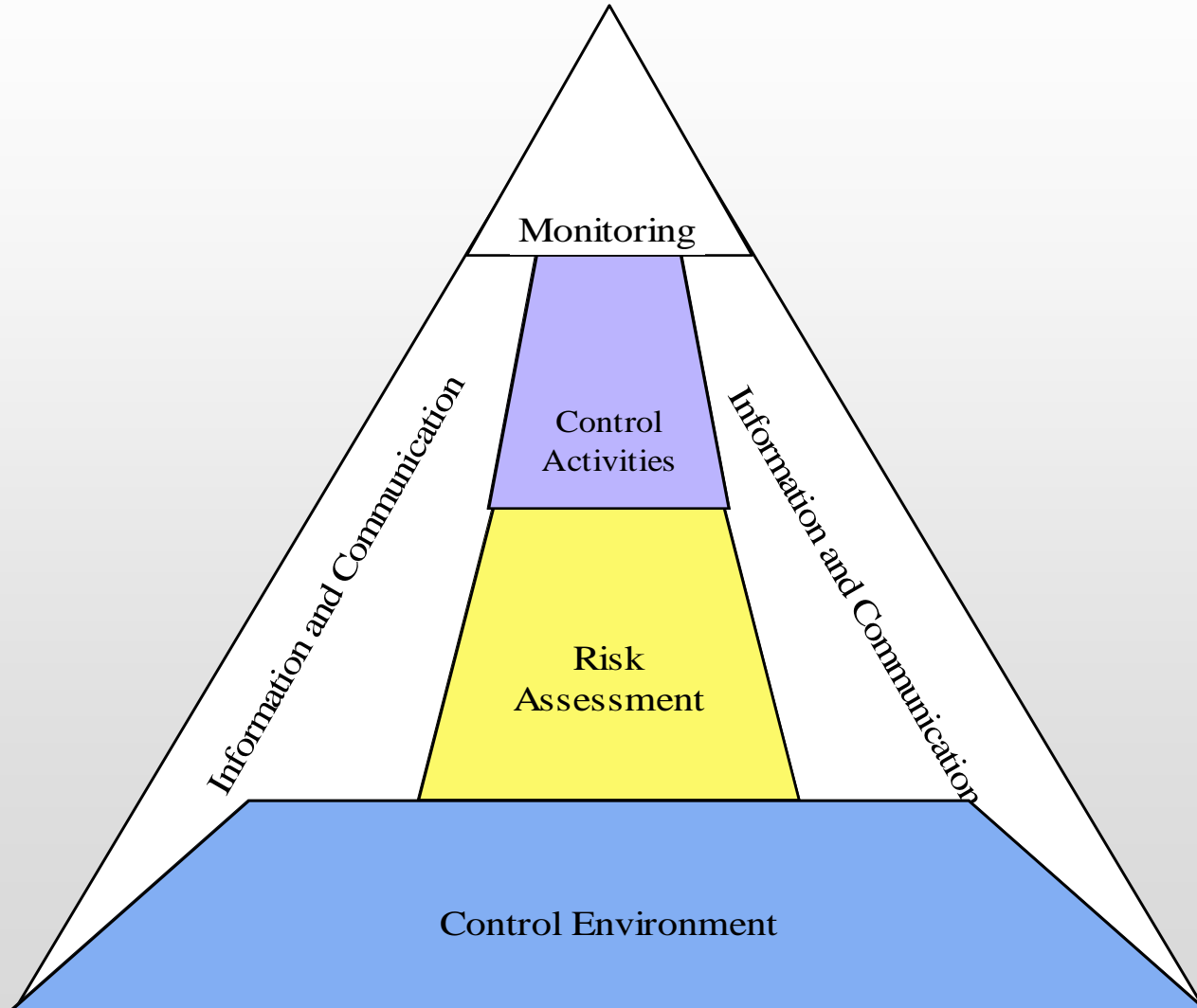
# COSO Diagram



# Risk Assessment

- Every organization faces a variety of risks from external and internal sources that must be assessed.
- Risk assessments include identifying, analyzing, and managing risks relevant to the achievement of the organization's objectives.

# COSO Diagram



# Control Activities

- Policies and procedures that help ensure management directives are carried out.
- Control activities occur throughout the organization, at all levels and in all functions.
- Include a wide range of activities such as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

# Levels of Control in COSO

## Governance and Control Environment

---

**Level 1  
Controls  
(Execution)**

During  
execution of  
event or  
transaction

**Level 2  
Controls  
(Supervisory)**

Immediately  
after execution  
of event or  
transaction

**Level 3  
Controls  
(Oversight)**

Soon after  
execution of  
event or  
transaction

**Level 4  
Controls  
(Int/Ext Audit)**

Pre and post-  
operations audit of  
execution of on-  
going assurance

# Levels of Controls

## **Level 1 Controls** and **Level 4 Controls**

### **(Execution Activities/Controls)**

- Embedded in day-to-day operations
  - Policies, procedures, segregation of duties, comparisons, and reconciliations
- Performed on every transaction/event
- Performed by the generators of the transaction/event
- Performed in real-time as the event or transaction is executed

### **(Internal/External Audit)**

- Audit of the design of controls
- Performed either before the transaction/event is originated or long after
- Performed on individual transactions/events for discovery only
- Performed by staff with no involvement in the operations

# Levels of Control

## Level 2 Controls and Level 3 Controls

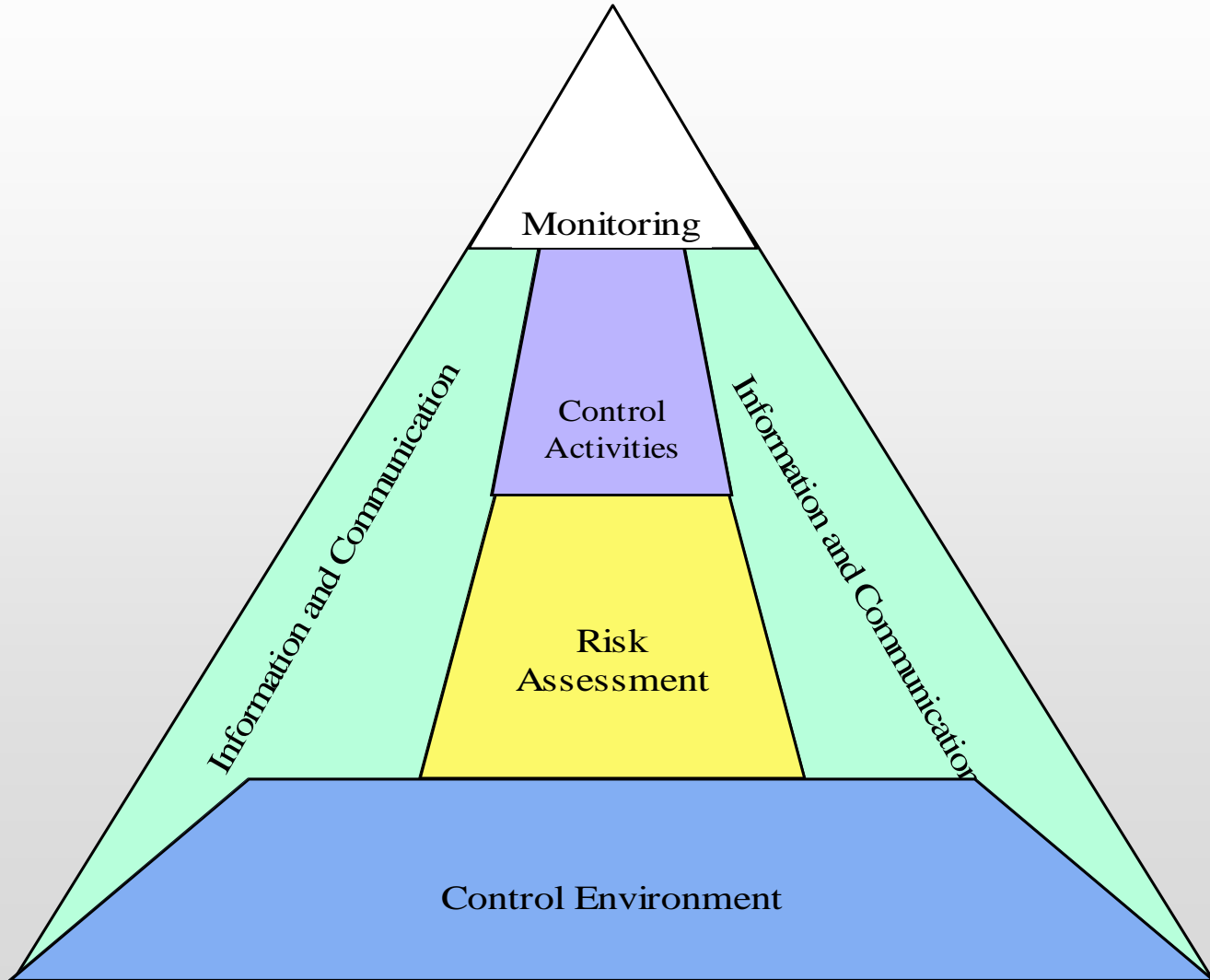
### (Supervision)

- Re-application of operating controls
  - Supervisory Review; Quality Assurance; Self Assessment
- Performed very soon after the generation of the event/transaction
- Performed by line management or staff positions who do not originate the event/transaction
- Performed on a sample of the total number of events/transactions

### (Oversight)

- Exception reports, status reports, analytical reviews, variance analysis
- Performed by representatives of executive management
- Performed on information provided by supervisory management
- Performed within a short period (weeks/months) after the event/transaction is originated

# COSO Diagram

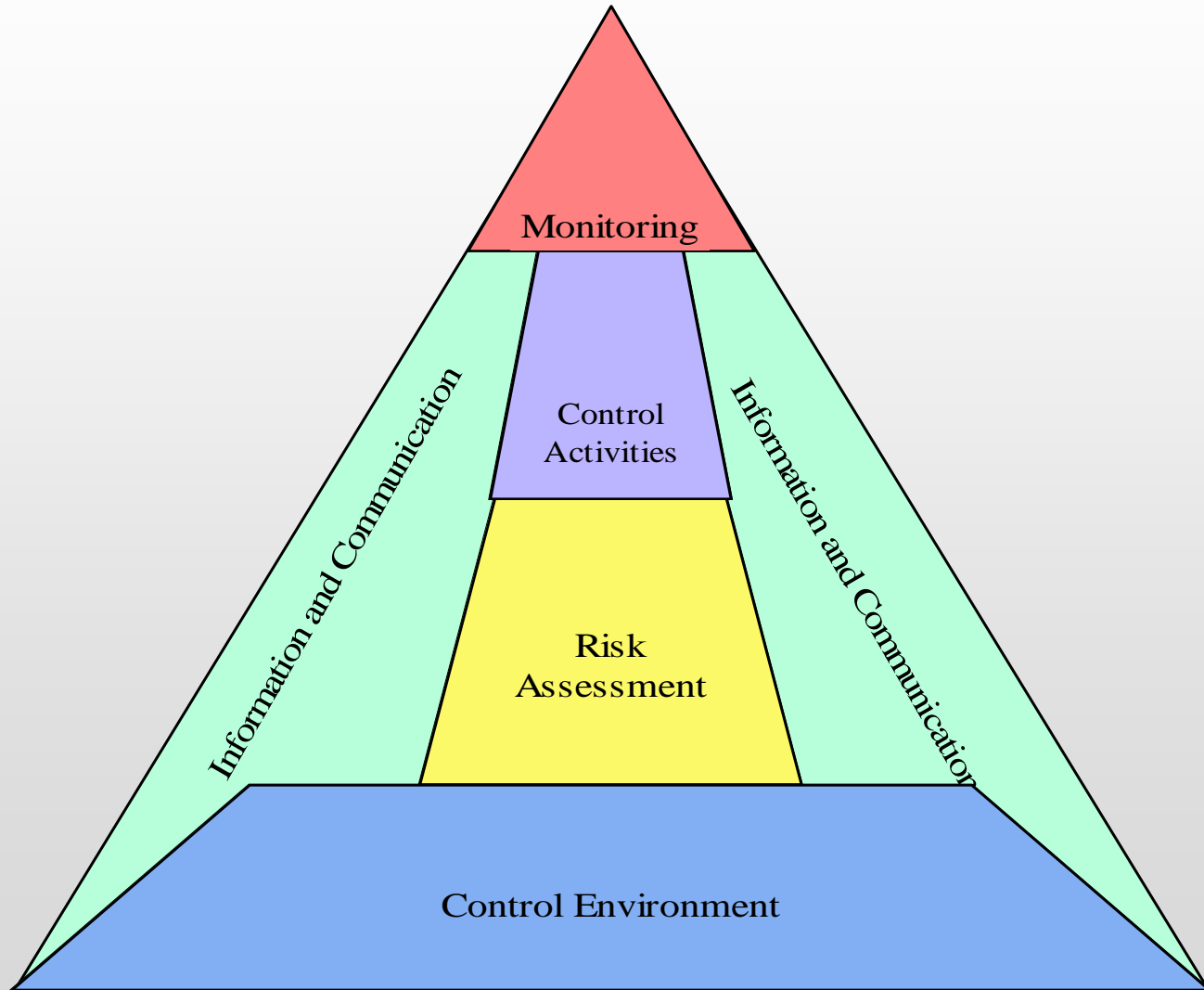


# Information and Communication

## **Ties other components together**

- Information is:
  - Delivered to people timely and in an useful format
  - Exchanged up, down, and across the organization and with external parties
  - Provided to help personnel understand their role in the internal control system and how their activities relate to the work of others

# COSO Diagram



# Monitoring

- Ensures that the internal control system continues to operate effectively
- Can be assessed through:
  - Ongoing monitoring activities such as regular management and supervisory activities; and/or
  - Separate evaluations such as self-assessments.
- Internal control deficiencies are reported to the appropriate management level

# Roles and Responsibilities

**Everyone in an organization has responsibility for internal control.**

- **Management** is directly responsible for internal controls.
- **Board of Regents** provides guidance and oversight.
- **Internal Auditors** evaluate the effectiveness of control systems, and contribute to ongoing effectiveness.
- **Other Personnel** are responsible for exercising due care in performing their duties and reporting any noncompliance with the code of conduct, or other violations of policy or illegal actions, to a higher organizational level.

# Limitations of Internal Control

- **Judgment** – managers can make bad decisions
- **Breakdowns** – people with control responsibilities may not carry them out effectively
- **Management Override** – a manager may intentionally go outside established practices for illegitimate purposes
- **Collusion** – two or more people can collaborate to subvert controls
- **Costs versus Benefits** – resources are limited. Managers properly accept a degree of risk when the cost of controlling that risk exceeds the benefit

# Fraud

## **Definition (Black's Law):**

- A known misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment.
- A misrepresentation made recklessly without belief in its truth to induce another person to act.
- A tort arising from a known misrepresentation made to induce another to act to his or her detriment.

# Occupational Fraud

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

# Elements of Occupational Fraud

- Activity is done in secret
- Violates the employee's duty of trust to the employer
- For the purpose of direct or indirect financial gain
- Organization loses assets, revenues, or reserves

# Common Fraud Schemes

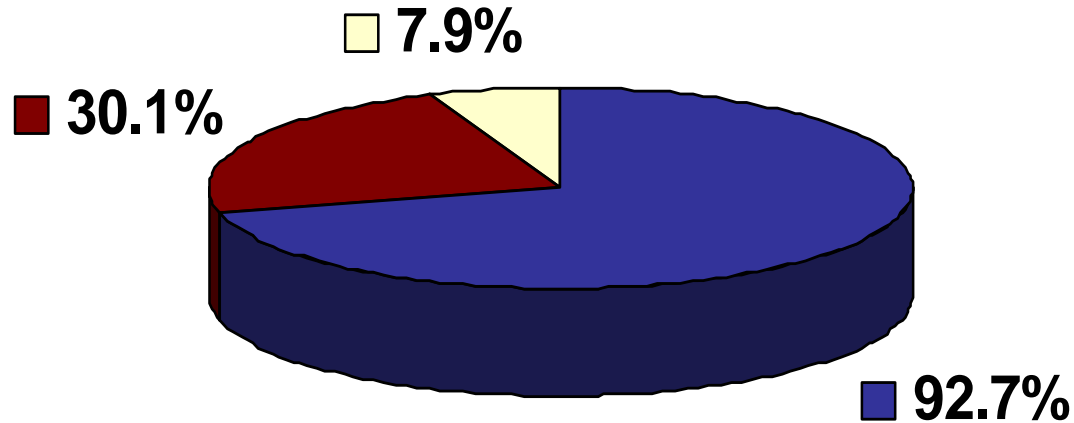
- Billing<sup>1</sup>
- Payroll<sup>1</sup>
- Expense reimbursement<sup>1</sup>
- Check conversion
- Journal entry manipulation
- Lapping of sales or receivables
- Skimming
- Incoming cash larceny
- Deposit larceny
- Fraudulent disbursement
- False refunds
- Fraudulent check coding
- Inventory shrinkage or inflation

<sup>1</sup> Leads to greatest rewards for the employee fraudster

# Common Fraud Schemes

- Stealing money/merchandise
- Kickbacks/bribery
- Falsifying internal reports
- Price-fixing
- Fraudulent financial reporting
- Software piracy/unauthorized use of computers
- Bid rigging
- Insider trading
- Computer crime
- Money laundering
- Credit card fraud
- Check fraud
- Insurance fraud
- Ghost employee schemes
- Overtime schemes
- Expense report schemes
- Over billing schemes
- “Dummy vendors” schemes
- Giving friends/relatives unauthorized services

# Fraud Schemes



■ Asset Misappropriation = 92.7%

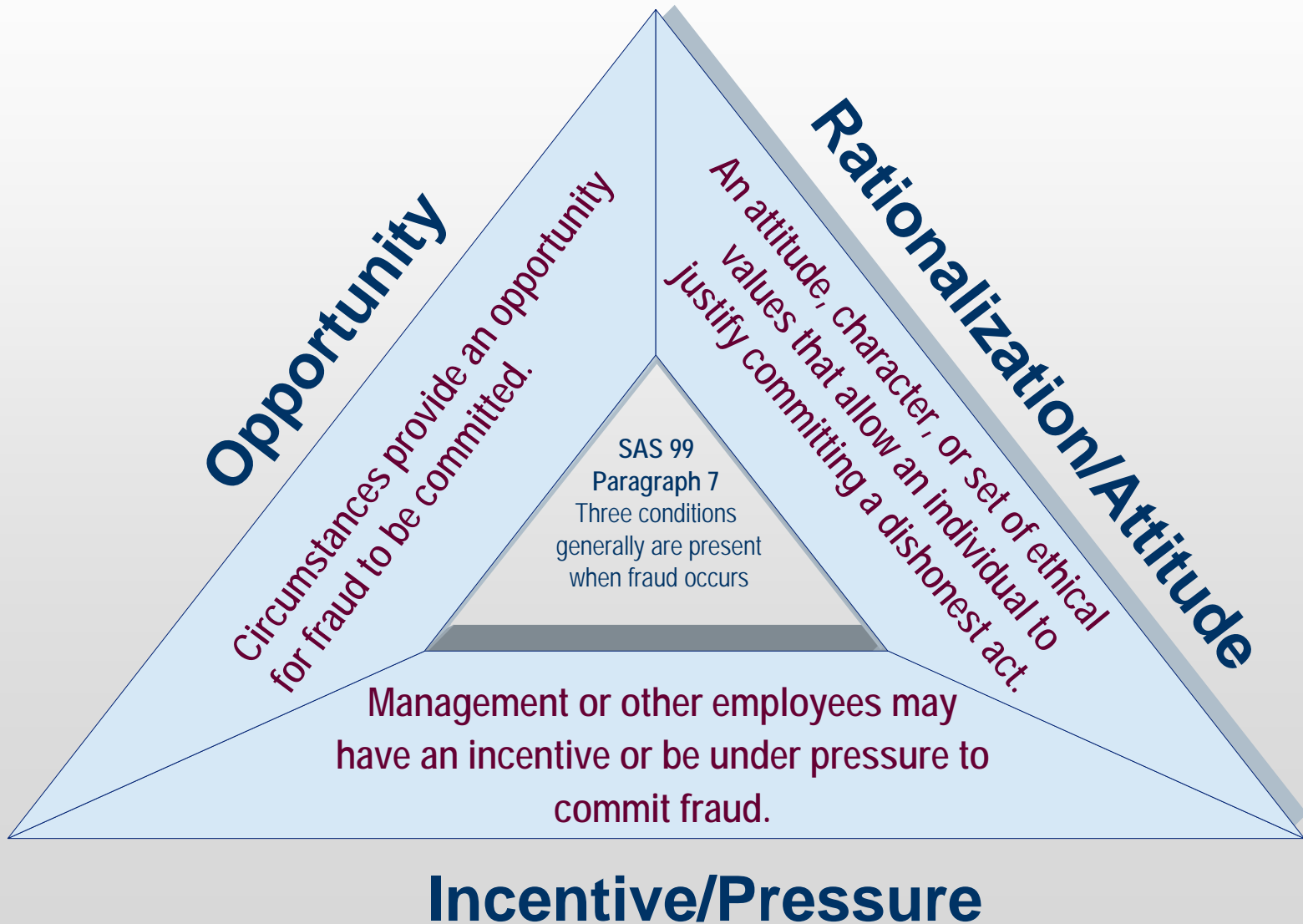
■ Corruption = 30.1%

■ Fraudulent Statements = 7.9%

Note: The sum of percentages in this chart exceeds 100% because a number of cases involved multiple schemes that fell into more than one category.

# The Fraud Triangle

(Source: State Auditor's Office)



# Common Excuses for Committing Fraud

- I was only borrowing the money
- It's not much, the organization won't miss it
- Everyone does it
- They owe me
- I'll stop once I get over this financial hump
- The organization mistreats me
- I haven't gotten a raise in years

# Preventing Fraud

- Most cost-effective way to deal with fraud is to prevent it through good internal controls
  - Put someone in charge
  - Create a culture of honesty
  - Adopt an ethics policy
  - Conduct a fraud risk assessment
  - Develop policies and procedures
  - Provide staff with training
  - Create a reporting mechanism for reporting irregularities (hotline)
  - Establish consequences

# Profile of an Embezzler

- Excellent attendance record
  - Comes to work even when very sick
  - Never takes a vacation
  - Willing to stay late and work weekends
- Performs job extremely well
- Always willing to take on additional responsibilities
- Is the “ideal”, “indispensable” employee

# The Perpetrator

- Need to balance oversight and trust
  - Most have no prior criminal history
  - Direct correlation between length of time employed with organization and size of loss
  - Higher level of authority
  - Greater degree of trust
  - More autonomy

# Detection of Frauds in Government Agencies

- Tip 48.5%
- Internal Audit 32.4%
- By Accident 14.7%
- Internal Controls 11.8%
- External Audit 5.9%
- Notified by Police 1.5%

Note: The sum of percentages in this chart exceeds 100% because in some cases respondents identified more than one detection method.

Source: 2004 Report to the Nation on Occupational Fraud and Abuse, Assoc. of Certified Fraud Examiners

# Tips by Source

- Reporting should reach out to customers, vendors, and other third party sources.
  - Employee 59.6%
  - Customer 19.7%
  - Vendor 15.7%
  - Anonymous 12.9%

Note: The sum of percentages in this chart exceeds 100% because in some cases tips were received from more than one source.

Source: [2004 Report to the Nation on Occupational Fraud and Abuse](#), Assoc. of Certified Fraud Examiners

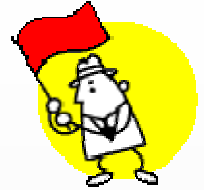
# Detecting Fraud

- Become knowledgeable about fraud schemes
- Know the warning signs (red flags or fraud indicators)
- Monitor
- Follow up on suspicions
- Take action when fraud is detected

# WARNING SIGNS of FRAUD

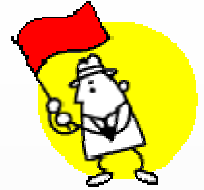
- Accounting irregularities
  - Documents altered
  - Documents falsified
  - Documents missing
- Rule breakers
- Big spenders
- People with financial problems

# Red Flags: Employees



- Marked personality changes in employees
- Financial pressure on employees
  - High personal debts
  - Great financial losses
  - Extensive gambling
- Key employees with too much control
- An employee living beyond his or her means
- Associations with vendors outside of normal working relationships
- Developing outside businesses closely associated with main employment

# Red Flags: Employees



- Extensive use of alcohol and drugs
- Significant personal or family problems
- Skipping vacations
- Extensive overtime
- Questionable background and references
- Extensive sick leave
- Expressed feelings that pay is not commensurate with responsibilities
- Strong desire to beat the system
- Regular borrowing of small amounts from fellow employees

# Red Flags: Transactions



- Unauthorized transactions
- Unexplained pricing exceptions
- Excessive payments to vendors
- Changes in purchasing norms
- Large petty cash transactions
- Inability to trace invoices
- Rising or unexplained department expenses

# Texas Penal Code

## **Section 31.03: Increases penalties for thefts committed by public servants.**

If the person committing the theft is:

- defined as a public servant at the time of the offense, and
- the stolen property came into the person's possession by virtue of his or her position,

Then, the punishment increases to the next highest category.

# Why Report Fraud?

**It is your responsibility as an A&M System employee.**

- Report dishonest, unethical or criminal activities that might affect any A&M System member such as:
  - Theft
  - Corruption
  - Misuse of System vehicles and/or equipment
  - Conflicts of interest

# Where to Report Fraud?

**Report suspected fraudulent incidents in accordance with System Policy 21.04 Control of Fraud and Fraudulent Actions.**

- Employee's supervisor;
- CEO; or
- Chief Auditor (System Internal Audit)
  - Fraud, Waste, and Abuse Hotline: (888) 501-3850
  - Website: <http://sago.tamu.edu/iaudit>

# Internal Controls/Fraud

## Contact Information:

- Charley B. Clark, Associate Vice President for University Risk and Compliance
  - [cbc@tamu.edu](mailto:cbc@tamu.edu)
  - 845-0977
  - <http://urc.tamu.edu>

Questions?