



MOORE STEPHENS
LOVELACE

New COSO Model and How Internal Controls Help to Reduce Opportunity for Fraud

Presented By
William Blend, CPA, CFE

Session Overview

- Review the new COSO model on internal controls.
- Discuss internal controls and their practical application.



Here We Go!



MOORE STEPHENS
LOVELACE



FRAUD HIGHLIGHTS

Recent Cases

City of Dixon, Illinois – Rita Crundwell, Comptroller, pleaded guilty to stealing more than \$53 million.

SEC Charges City of South Miami with Defrauding Investors – City charged with defrauding investors related to the tax-exempt status of municipal bonds.



Recent Cases

Broward County – Two executives with a traffic equipment company sentenced to prison for bribing a Broward County employee in the Traffic and Engineering Department.

Osceola Tax Collector Employee – Employee accused of providing more than 200 Florida licenses to illegal immigrants.



Who's Responsible for Internal Controls

Savage Chickens

by Doug Savage



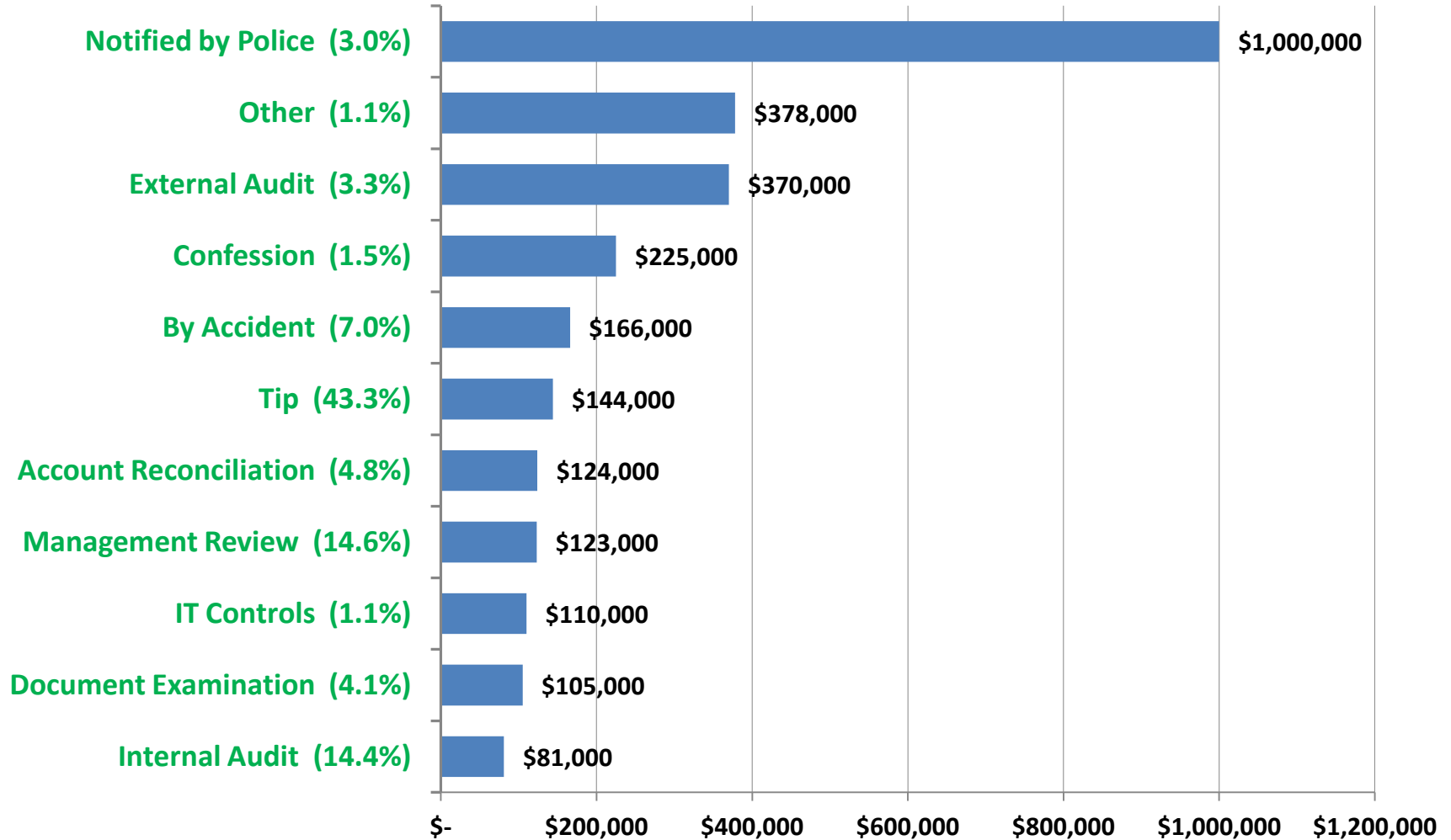
www.savagechickens.com



MOORE STEPHENS
LOVELACE

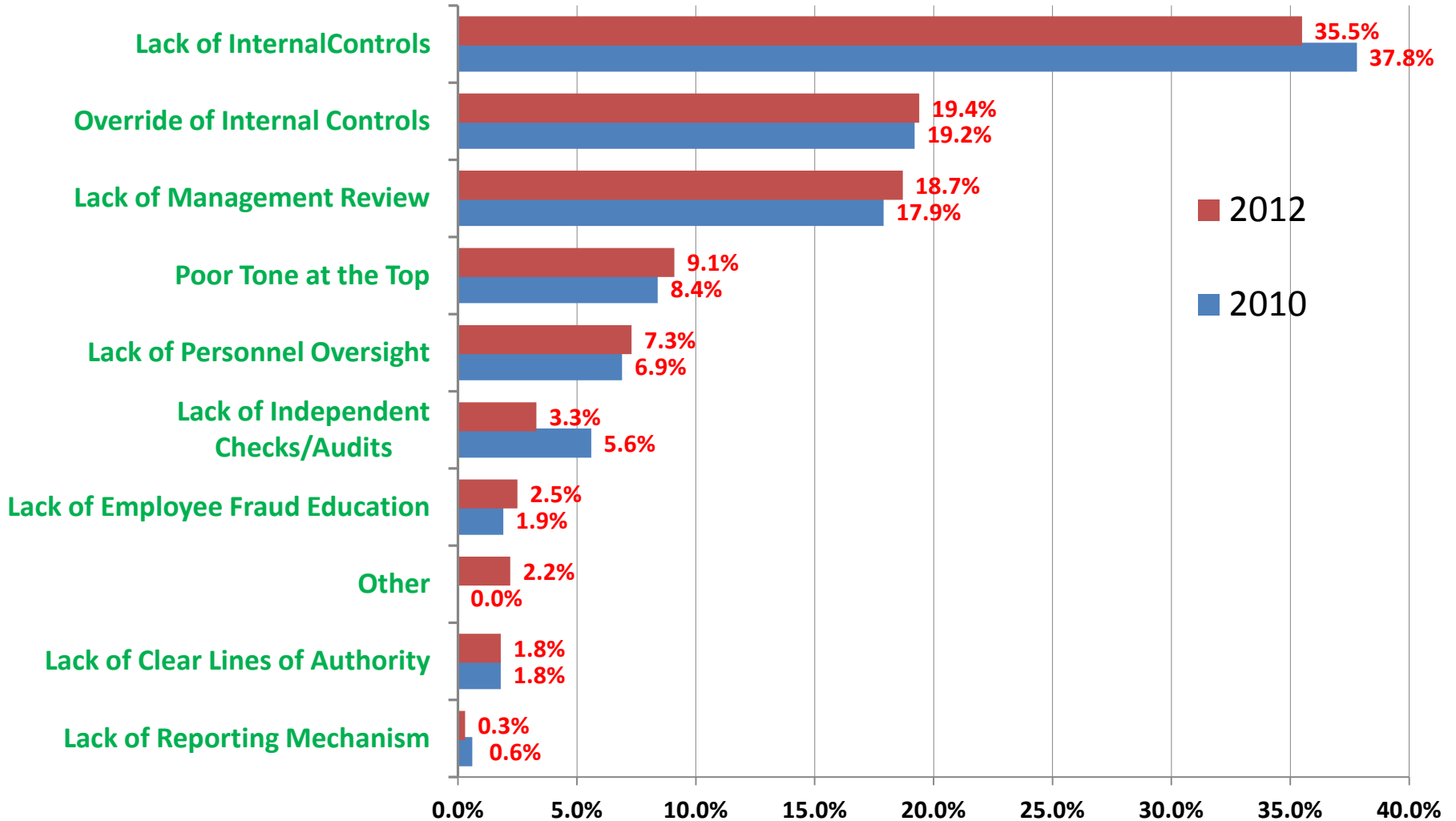
ACFE Report to Nations Data

Detection Method (% Cases) and Median Loss 2012



ACFE Report to Nations Data

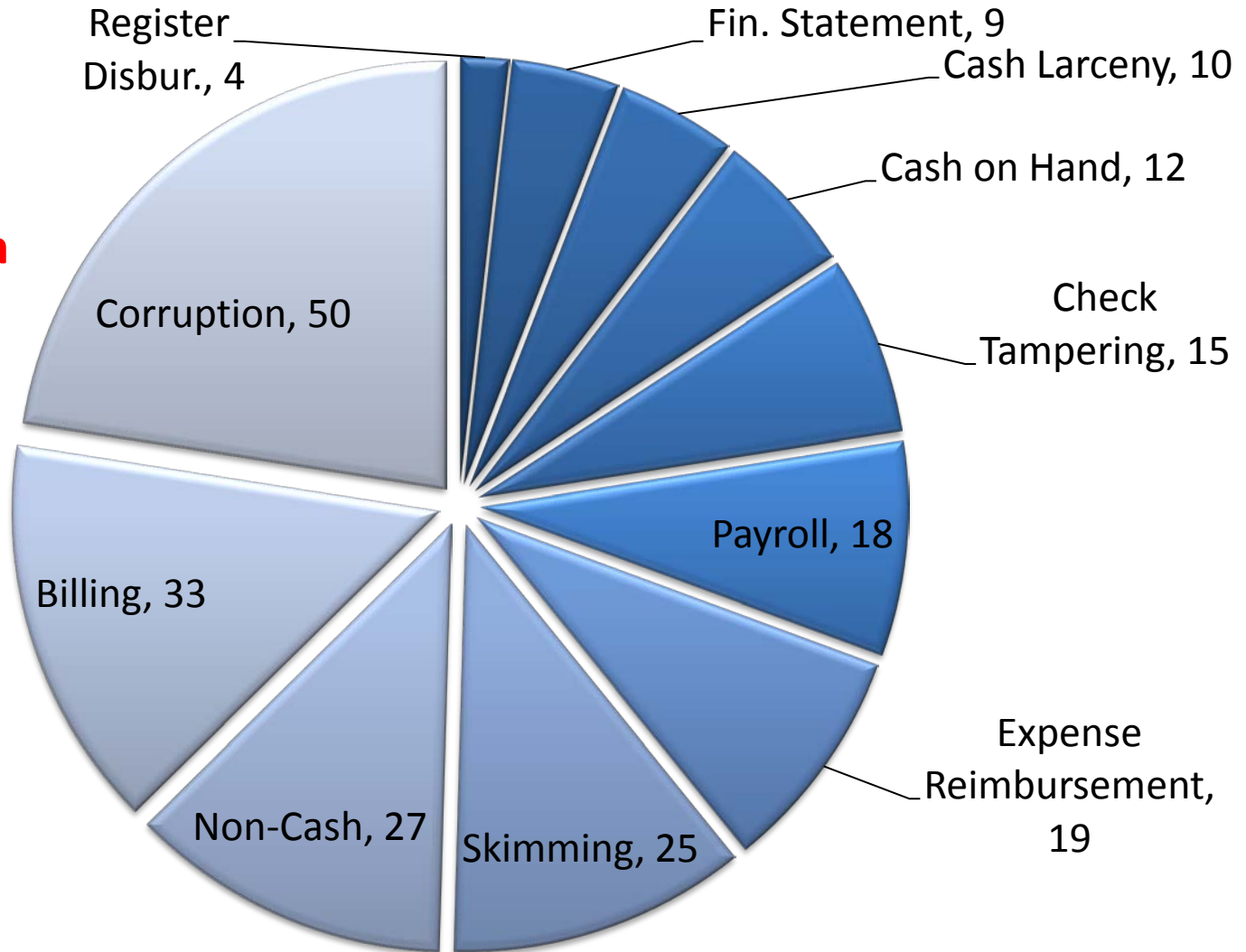
Primary Internal Control Weakness Observed



ACFE Report to Nations Data

Primary Internal Control Weakness Observed

**Number
Cases (141)
Govt. &
Public Admin**



Stay With Me Now



MOORE STEPHENS
LOVELACE



INTRO TO NEW COSO FRAMEWORK

New COSO Model

Why Should I Care About The New COSO Model?

- The strongest prevention and detection tools to help prevent fraud are strong internal controls.
- COSO is accepted as a leading framework for designing, implementing, and conducting internal controls and assessing the effectiveness of internal controls.



New COSO Model

Why update the 1992 COSO Model?

- Change in business models. They have become more complex, increased outsourcing, joint ventures, and globalization.
- Increased stakeholder (governance, audit committees, the public and regulators, etc.) expectations seeking more transparency and accountability for the integrity of IC systems. They expect the organization's IC system to protect its resources from fraud.
- Technology advances. In 1992, while technology (such as the internet, e-mail, etc.) was present, its business use has significantly expanded. Think of cloud computing, data hosting, mobile technology (laptops, cell phones, tablets), etc.



New COSO Model

Transition Period

- The original framework will be made available during a transition period extending to December 15, 2014.
- Transition period is May 14, 2013 through December 15, 2014. During that period, the COSO Board believes organizations should clearly disclose which framework they are relying on in any external reporting.



New COSO Model

What stays the same?

- Core definition of internal control and the five components (Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring).
- The requirement to consider the five components in assessing the effectiveness of an internal control system remains “fundamentally” unchanged.
- The framework continues to emphasize management’s judgment in designing, implementing and conducting internal control, as well as the assessment of its effectiveness.



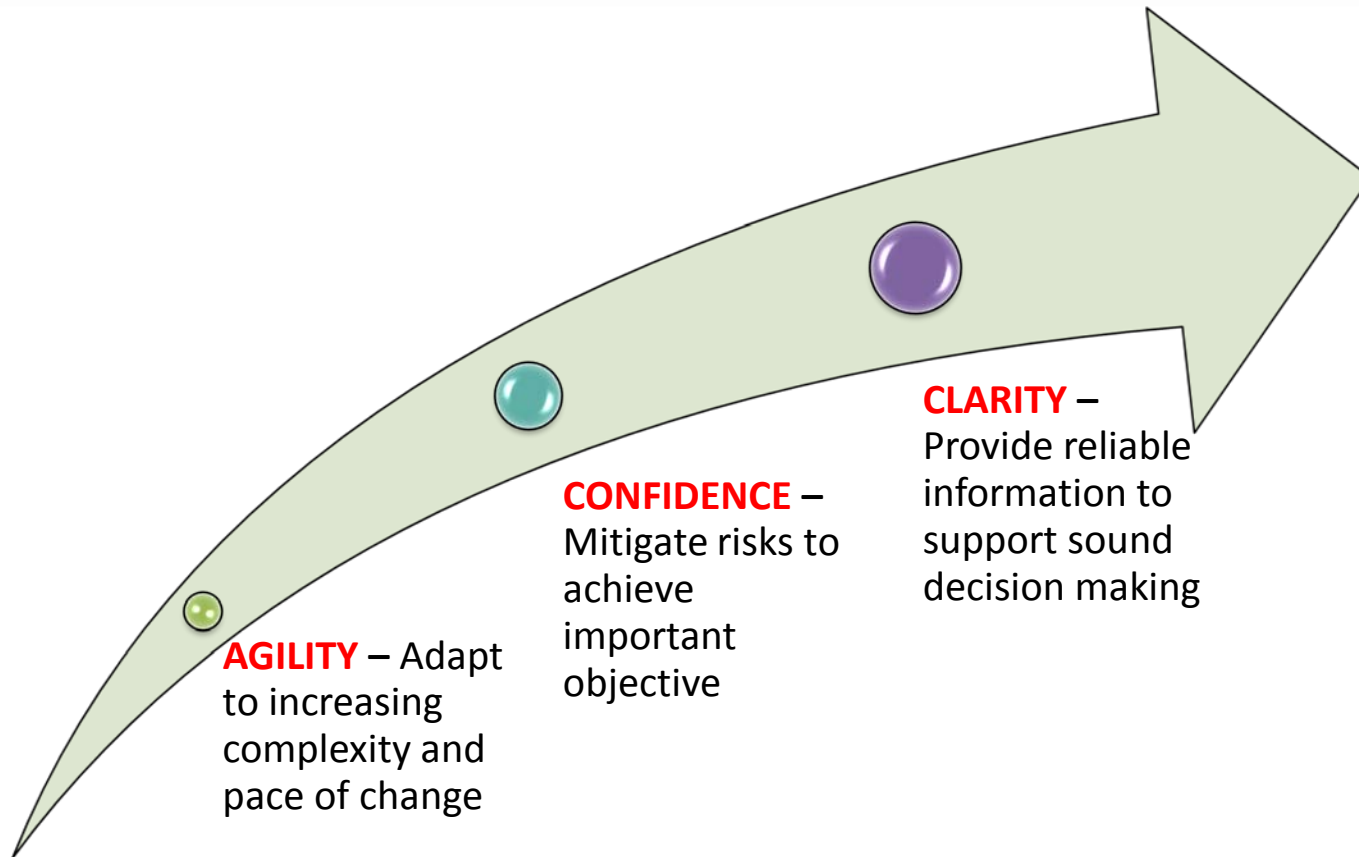
New COSO Model

What's new?

- Enhancements and clarifications that are intended to ease use and application.
- Formalization of fundamental concepts introduced in the original model are now principles in the new model. Each principle has a subset of 82 associated “points of interest”.
- Framework is expanded to include other important forms of reporting, such as non-financial and internal reporting.



New COSO Model



**THE UPDATED
FRAMEWORK
BETTER
SUPPORTS
EFFORTS TO
DESIGN AND
ADAPT
SYSTEMS OF
INTERNAL
CONTROL**





NEW COSO CUBE

THE COSO CUBE

Objectives, Components and Principles:

- An organization adopts a mission and vision, sets strategies, establishes objectives it wants to achieve, and formulates plans for achieving them.
- Objectives may be set for an entity as a whole or targeted to specific activities within the entity. Though many objectives are specific to a particular entity, some are shared (i.e., sustaining organizational success, reporting to stakeholders, recruiting and retaining motivated and competent employees, achieving and maintaining a positive reputation, and complying with laws and regulations)



THE COSO CUBE

Objectives, Components and Principles (cont.):

- The five components (Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities) of internal control support the organization's objectives.
 - Three categories of objectives; Operations, Reporting and Compliance (Cube's - Columns)
 - Five Components of internal control (Cube's - Rows)
 - Entity Structure (Cube's - Third Dimension)



THE COSO CUBE

THEN



NOW





USERS OF THE FRAMEWORK



New COSO Model

Ways management and governance may utilize the New Framework:

- Apply framework at various organizational levels (operating unit, function, etc.)
- Means to identify and analyze risk and develop appropriate responses, including a greater focus on anti-fraud measures
- Expanded application from financial reporting to operations and compliance objectives
- Opportunity to remove ineffective and redundant controls that provide minimal value to the organization



New COSO Model

Ways third parties gain value from the New Framework:

- Confidence in governance oversight of internal control systems
- Confidence regarding the achievement of an organization's goals
- Confidence in the organization's ability to identify, analyze, and respond to risk and changes in the business and operating environment
- Increased understanding of the requirements for an effective internal control system
- Greater understanding of management's use of internal controls to operate more efficiently and reduce redundancies in controls





COSO COMPONENTS AND PRINCIPLES



New COSO Model

The Framework views all components of internal control as suitable and relevant to all entities:

- Principles are fundamental concepts associated with components. As such, the Framework views the seventeen principles as suitable to all entities. The Framework presumes that principles are relevant because they have a significant bearing on the presence and functioning of an associated component. Accordingly, **if a relevant principle is not present and functioning, the associated component cannot be present and functioning.**



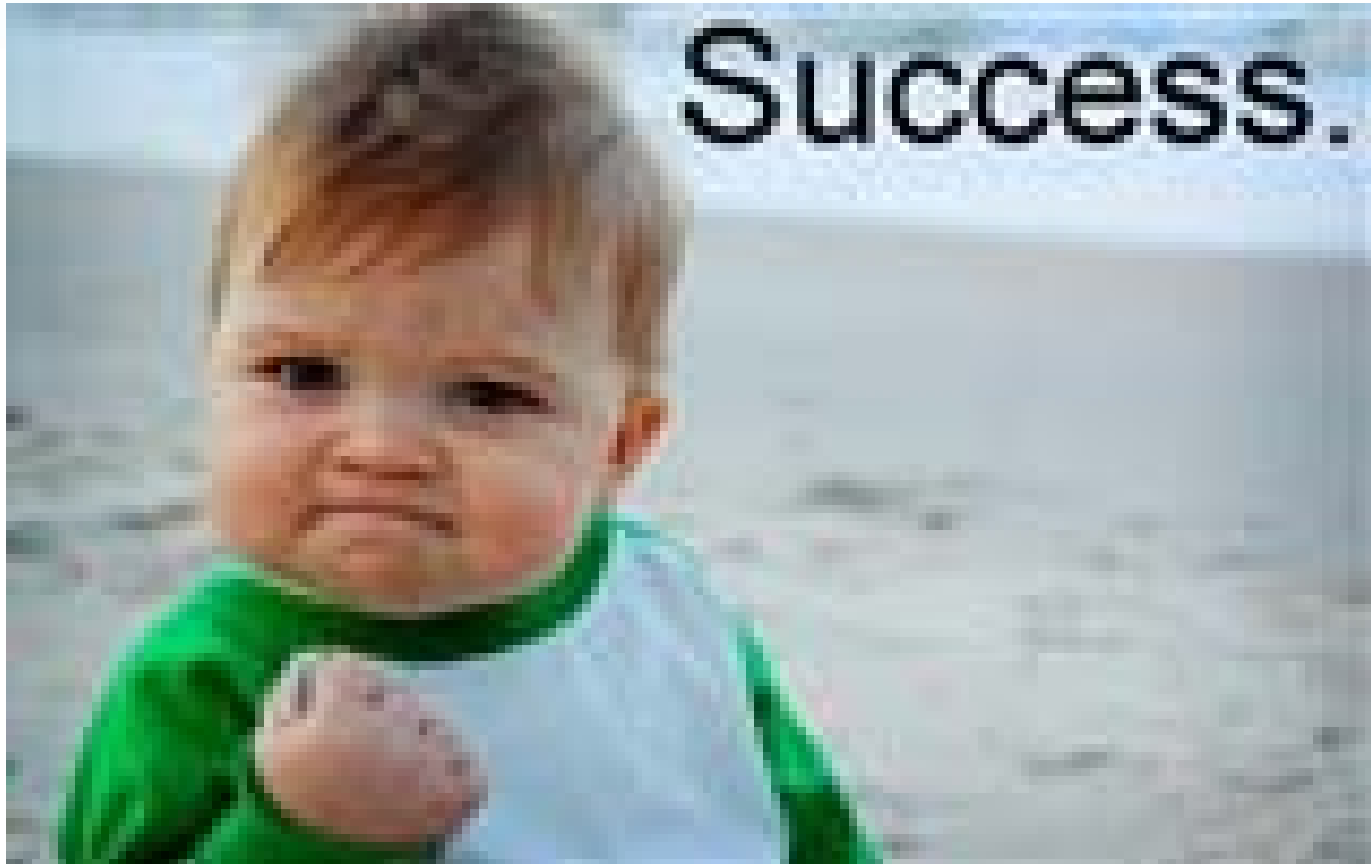
New COSO Model

What is meant by “Present” and “Functioning”?

- **Present** - determination that components and relevant principles **exist in the design and implementation** of the system of internal control to achieve specified objectives
- **Functioning** - determination that components and relevant principles **continue to exist in the conduct** of the system of internal control to achieve specified objectives



New COSO Means Success, Baby



MOORE STEPHENS
LOVELACE

Buy In or I'll Knock Your Block Off



MOORE STEPHENS
LOVELACE

Principles

Control Environment - Component

- 1) Demonstrates commitment to integrity and ethical values
- 2) Exercises oversight responsibility
- 3) Establishes structure, authority and responsibility
- 4) Demonstrates commitment to competence
- 5) Enforces accountability



Principles (continued)

Risk Assessment - Component

- 6) Specifies relevant objectives
- 7) Identifies and analyzes risk
- 8) **Assesses fraud risk**
- 9) Identifies and analyzes significant change



Principles (continued)

Control Activity - Component

- 10) Selects and develops control activities
- 11) Selects and develops general controls over technology
- 12) Deploys through policies and procedures



Principles

Information and Communication - Component

- 13) Uses relevant information
- 14) Communicates internally
- 15) Communicates externally



Principles (continued)

Monitoring Activities - Component

- 16) Conducts ongoing and/or separate evaluations
- 17) Evaluates and communicates deficiencies



Principles (continued)

Monitoring Activities - Component

- 18) Conducts ongoing and/or separate evaluations
- 19) Evaluates and communicates deficiencies

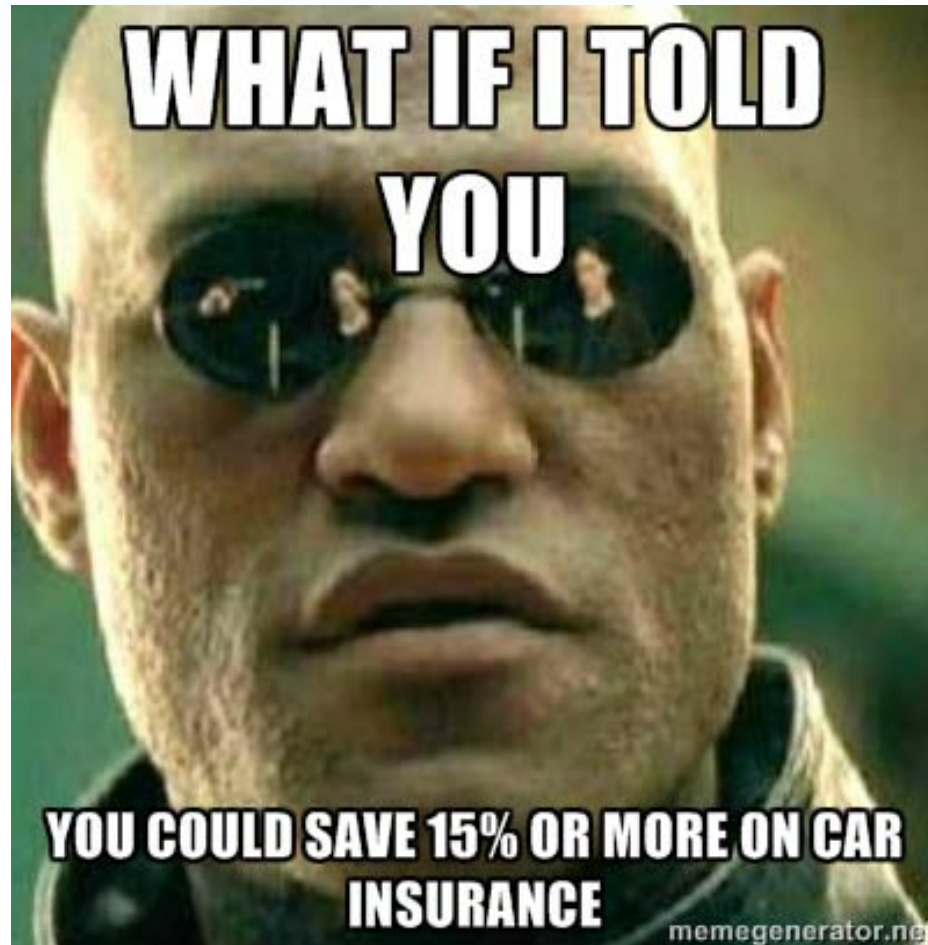




COSO POINTS OF FOCUS



Matrix Morpheus Asks



MOORE STEPHENS
LOVELACE

Points of Focus - Example

Principles Associated with Monitoring Activities and Related Points of Focus:

16) Conducts ongoing and/or separate evaluations – associated points of interest:

- Consider a Mix of Ongoing and Separate Evaluations
- Consider Rate of Change
- Establish Baseline Understanding
- Use Knowledgeable Personnel
- Integrate with Business Processes
- Adjust Scope and Frequency
- Objectively Evaluate



Points of Focus - Example

Principles Associated with Monitoring Activities and related Points of Focus (continued):

17) Evaluates and communicates deficiencies:

- Assess Results
- Communicate Deficiencies
- Monitor Corrective Actions



Principal 8 - Potential Fraud Risk

Principle 8 – The organization considers the potential for fraud in assessing risks to the achievement of objectives.

Points of Focus under Principle 8:

- Considers various types of fraud
- Assesses incentives and pressures
- Assesses opportunities
- Assesses attitudes and rationalizations



Principal 8 - Potential Fraud Risk

Principle 8 – Is this new????





COSO 2013 AND TECHNOLOGY

New COSO Model and Technology

Principle 11 states - *“The organization selects and develops general control activities over technology to support the achievement of objectives.”*

Related points of focus:

- **Determine dependency between the use of technology in business processes and technology's general controls.**



New COSO Model and Technology

Principle 11 related points of focus (cont.):

- Establishes relevant technology infrastructure control activities.
- Establishes relevant security management process control activities.
- Establishes relevant technology acquisition, and maintenance process control activities.



New COSO Model and Technology

- **Essential to support the entities' objectives.**
- **Various terms are used to identify - such as management information systems, information technology. The framework uses technology in referring to computer systems, including software applications and operational control systems.**



New COSO Model and Technology

- **Environments vary in size, complexity and extent of integration**
- **Creates both opportunities and risks**
- **The framework principles do not change with the application of technology**





TRANSITION TO NEW MODEL



Transition to New Model

Develop a transition plan. Don't wait for your auditors to start making comments stay ahead of the curve!

- Develop an awareness of the model within your organization with key implementation personnel.
- Evaluate how your current controls will need to be updated, the impact of any "new" requirements and the resources needed to address them.
- Inform and include governance in the process.
- Execute your plan and continually review and improve.



Transition to New Model

Keep in front of your auditors:

- Most likely the model will be implemented in the public company sector first.
- Like Sarbanes Oxley the related internal control requirements (COSO) filtered to governments.
- Remember that if a Principal is not present and operating effectively than the related component is not.



Transition to New Model

Work with your auditors:

- Most likely the audit standards will need to be updated to incorporate the principals.
- Your external auditor can assist in the evaluation of your plan and the related implementation.
- Communication will be the key to ensuring that there are no “surprises”.





PRACTICAL DISCUSSION OF INTERNAL CONTROLS

Internal Control Myths and Facts

Myth

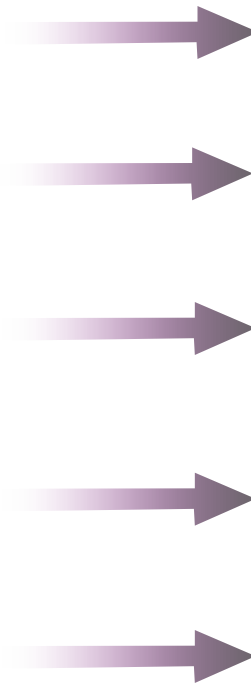
Starts with a strong set of policies and procedures.

Internal auditors are responsible for internal controls.

It's an accounting thing; we do it because they tell us to.

Takes time away from our core activities.

Strong controls will prevent fraud.



Fact

Starts with a strong control environment.

Management is the owner of internal control.

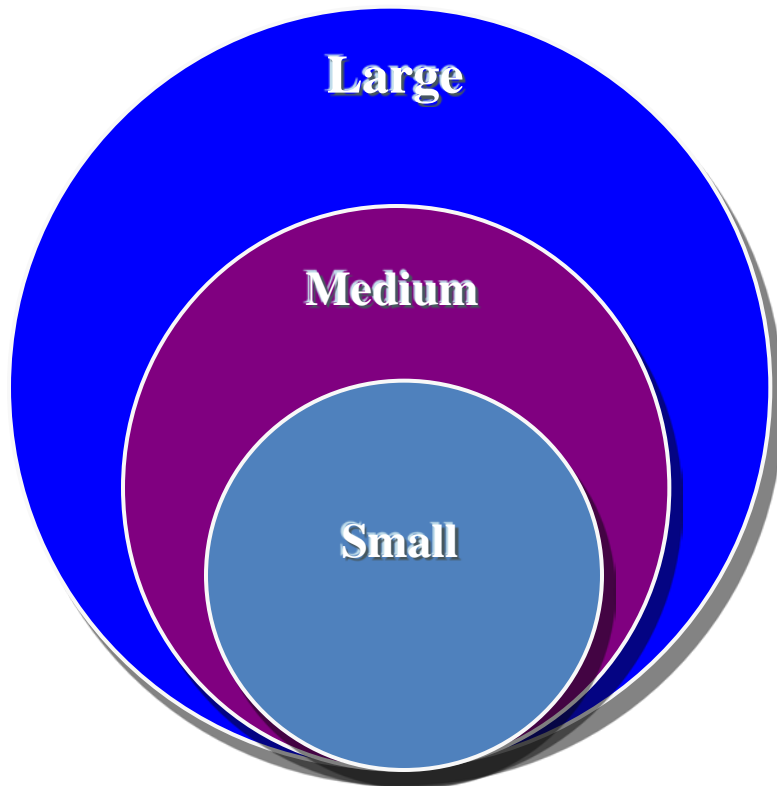
It's everyone's responsibility and should be an integral part of operations.

Should be built into, not on to business processes.

Controls provide reasonable, but not absolute assurance.

Internal Controls and Resources

Size = Resources



**Good Segregation of Duties
Internal Audit Function
More degreed personnel**

**Good Segregation of Duties
No Internal Audit Function
Fewer degreed personnel**

**Lack of Segregation of Duties
No Internal Audit Function
No degreed personnel**

Internal Controls

- **What are internal controls?**

Put simply, they are an exercise in common sense mixed with a healthy lack of trust!

- You use them in your everyday life:

- Balance your checkbook
- Lock up your car and home
- Review your personal credit card statements



Internal Controls

- At an organizational level, they are vital to ensure:
 - Resources are protected against fraud, waste and abuse
 - Accurate reporting and reliability of financial and operational information
 - Proper evaluation of personnel and business performance



Internal Controls

- Things to remember about internal controls:
 - They are a processes with a means to an end, not an end to itself
 - Effected by people and technology
 - Only provide reasonable assurance
 - Must be evaluated on a cost-benefit basis



Internal Controls

- Things to remember about internal controls and the new model:
 - Controls and evaluation utilizing the new model should not just be a financial process
 - Operational controls should be evaluated utilizing the model
 - Controls implemented to ensure legal and regulatory compliance should be evaluated utilizing the model
 - Remember – operational, internal and other periodic financial informational reporting



Internal Controls

- Implementation:
 - Create policies and procedures that help to ensure that actions necessary to achieve the organization's objectives are effectively carried out. Utilize the framework in developing new policies and procedures and reviewing/updating current policies and procedures.



Internal Controls

- Implementation:
 - Formalize your policies and procedures (written and approved by governance) and communicate them to all members of the organization.
 - Train employees to understand how to properly implement policies and procedures and emphasize their importance.



Internal Controls

- Implementation:
 - Cost benefit analysis
 - Continued employee buy in
 - A rubber stamp control is no control at all
 - Employees are people. If internal controls makes sense and employees have a say, employees will follow and perform the control.



Internal Controls

- Implementation:
 - There are 5 components of internal control
 - Two (2) tend to be most overlooked - Risk Assessment and Monitoring



Internal Controls

- Implementation (Risk Assessment):
 - Do you do it?
 - Should be performed at least annually and more frequently if there are significant changes in your organization
 - Document the process
 - Include key members of your organization
 - Don't make it a formality



Internal Controls

- Implementation (Monitoring):
 - Do you do it?
 - Generally it is an ongoing process
 - Do you document?
 - While certain “controls” may have a built-in monitoring component, entity-wide monitoring should occur.

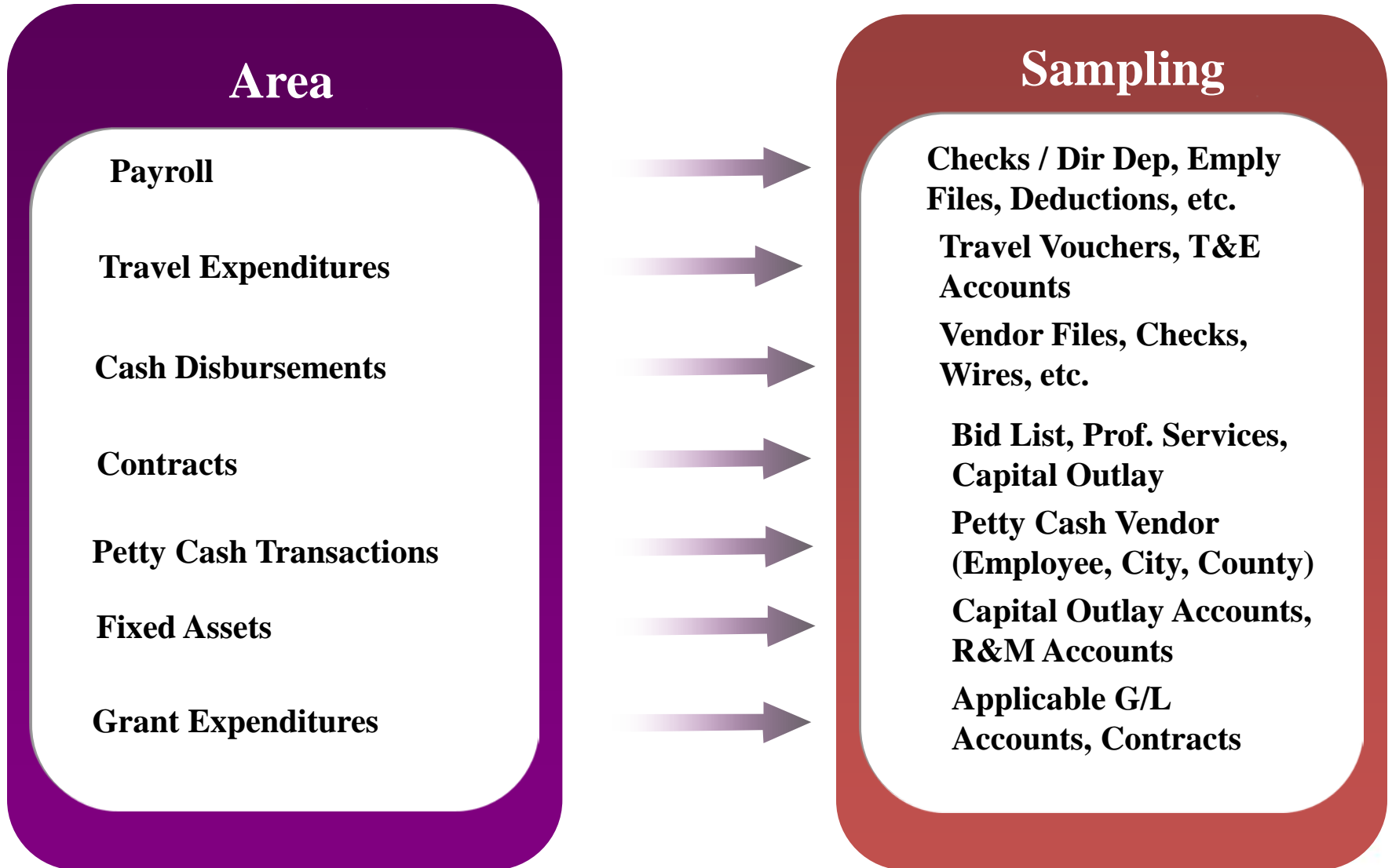


Internal Controls – Have You Considered

- Sampling doesn't just have to be for your auditor. Consider using it in your risk assessment and monitoring procedures.
 - Current technology allows organizations to utilize this tool
 - It's a simple process
 - Can be done quickly
 - Can be used in almost any process



Examples of Where Your Organization Could Consider Sampling



- Tone at Top
- Policies and procedures
- Organizational Authority

Control Environment

- Risk Assessment Meetings
- Identify Risks
- Address Risks

Risk Assessment

- Purchasing limits
- Approvals
- Reconciliations
- Specific P&Ps

Control Activities

- Distribution of P&Ps
- Communicate Ethics Policy
- Meetings to update on organizational progress

Information and Communication

- Monthly Management Reviews
- Unpredictable Reviews
- Internal Auditor Reviews

Monitoring



So What Do We Know About Internal Controls



MOORE STEPHENS
LOVELACE



WHY DO INTERNAL CONTROLS FAIL?



Internal Controls

- With all this emphasis, why do controls fail?
 - Inadequate knowledge of policies and procedures or governing regulations
 - Inadequate segregation of duties
 - Inappropriate access to assets
 - Rubber stamping controls - *“I just do it because I have to”.*



Internal Controls

- With all this emphasis, why do controls fail?
 - Override of controls
 - Collusion
 - Not understanding or ignoring red flags
 - Improper tone from the top
 - Complacency
 - Can you think of any others?





QUESTIONS?

