

**Office of Operations
2015 Fall Conference
December 8-9**

Partners in Excellence

RISK ASSESSMENT 101

Anna Tomassacci, Jaimie Corvetti, Adriana Alfeo



Office of the New York State Comptroller
Thomas P. DiNapoli, Comptroller

Office of Operations

John Traylor, Executive Deputy Comptroller

Division of Contracts and Expenditures

Margaret Becker, Deputy Comptroller

Bernie McHugh, Director, Bureau of State Expenditures

OBJECTIVES

- Perform a basic risk assessment
- Design a system of internal controls



AGENDA

- Risk Assessment Game
- Internal Controls Overview
- Group Exercise:
 - Perform a Basic Risk Assessment for Procurement and Accounts Payable Departments
 - Rank risks in terms of impact and likelihood
 - Create Risk Matrix
- Risk Assessment Trivia Game
- Prizes!



LET THE GAMES BEGIN!



COSO

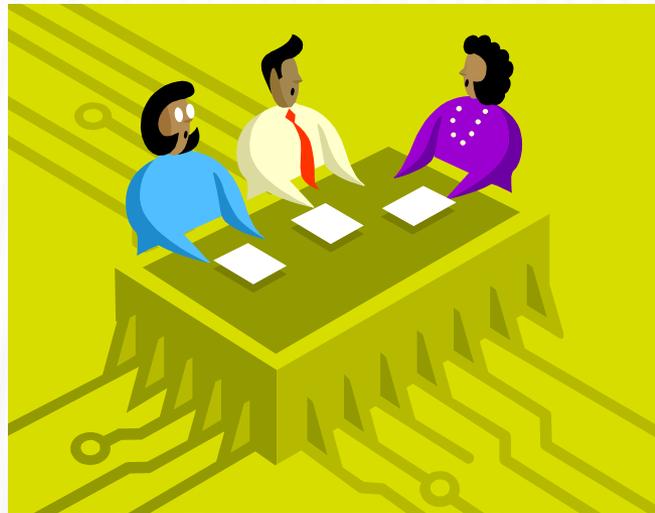
Committee of Sponsoring Organizations of the Treadway Commission (COSO)

A voluntary private sector organization dedicated to improving the quality of financial reporting to business ethics, effective internal controls, and corporate governance. Developed our current integrated framework in 1992.



INTERNAL CONTROL

- Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.



FUNDAMENTAL CONCEPTS

- Geared to the achievement of objectives in one or more categories
- A process consisting of ongoing tasks and activities
- Effected by people
- Able to provide reasonable assurance
- Adaptable to the entity structure

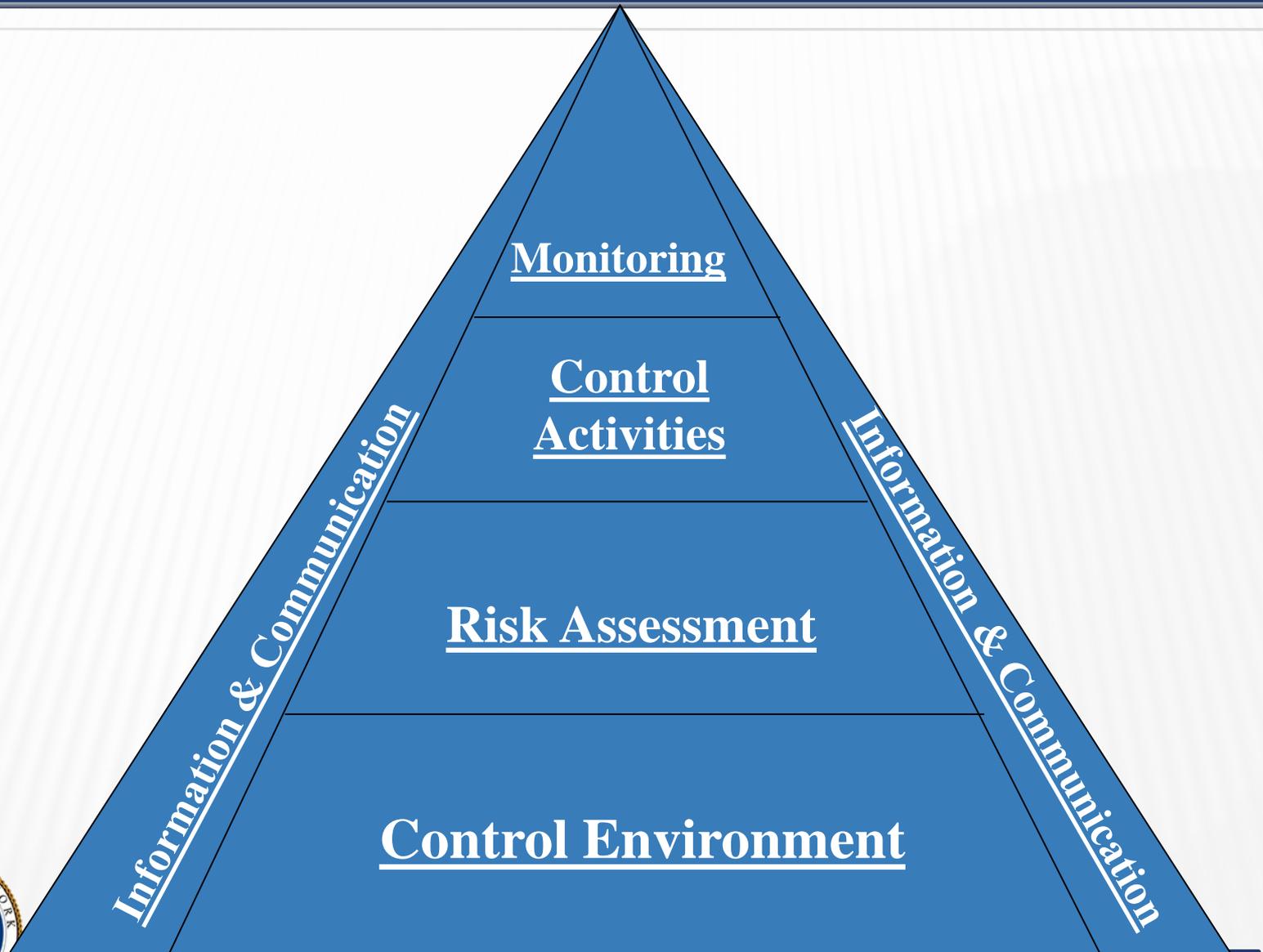


OBJECTIVES

- **Operations Objectives** – These pertain to effectiveness and efficiency of the entity’s operations, including operational and financial performance goals, and safeguarding assets against loss.
- **Reporting Objectives** – These pertain to internal and external financial and non-financial reporting and may encompass reliability, timeliness, transparency, or other terms as set forth by regulators, recognized standard setters, or the entity’s policies.
- **Compliance Objectives** – These pertain to adherence to laws and regulations to which the entity is subject.



THE PYRAMID



Risk

The possibility that an event will occur and adversely affect the achievement of objectives

Assessment

To evaluate; to examine carefully; to determine or set the value of something



RISK ASSESSMENT PROCESS

1. Identify your **objectives** (operations, reporting, compliance).
2. What could get in the way of achieving your **objectives**? What are the **risks**?
3. What is the likelihood of **the risks** occurring?
4. What is the impact if **the risks** do occur?
5. Is there a potential for **fraud**?
6. What **controls** are already in place?
7. Prioritize **the risks** and determine your next steps.



ASK THE QUESTIONS ...

- What obstacles could stand in the way of achieving your objective?
- What can go wrong?
- What is the worst thing that *could* happen?
- What is the worst thing that *has* happened?



ASK THE QUESTIONS ...

- Are there new processes? Changed ones?
- New goals or legislation?
- Staffing changes?
- What keeps you awake at night?



RISK ASSESSMENT

Assess each risk in terms of:

- The likelihood of the negative event
- The significance or impact of the event



RISK ASSESSMENT

Likelihood

The probability that an unfavorable event would occur if there were

1. no internal controls
2. existing internal controls

Impact

A measure of the magnitude of the effect on an organization if the unfavorable event were to occur



EVALUATING RISK

HIGH

L
I
K
E
L
I
H
O
O
D

LOW

Area II
Minimal
Concern

Area IV
Most Concern

Judgment
Required

Area I
Least Concern

Area III
Moderate
Concern

LOW

IMPACT

HIGH



THINGS TO KEEP IN MIND

- Change is the one constant
- A risk assessment is never “done”
- Communication and education can make all the difference
- The greatest risk is turning a blind eye to the possibility of risk
- Knowledge is power!



Three options:

- Avoid the risk
- Accept it
- Prevent it



MANAGING RISK

Avoid the risk:

Whatever the risky activity is...

Don't do it!

No additional controls are required



MANAGING RISK

Accept the risk:

Continue the way you're going

Maintain the Status Quo

No changes, no new controls



MANAGING RISK

Prevent or reduce the risk:

Actively work to control the risk

Change how you operate!

Establish whatever controls are necessary to manage the risk



CONTROL ACTIVITIES

The actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.



CONTROL ACTIVITIES

Controls can be...

- **Directive**: guide an organization toward desired outcome.
- **Preventive**: deter the occurrence of an undesirable event.
- **Detective**: identify undesirable events and alert management.

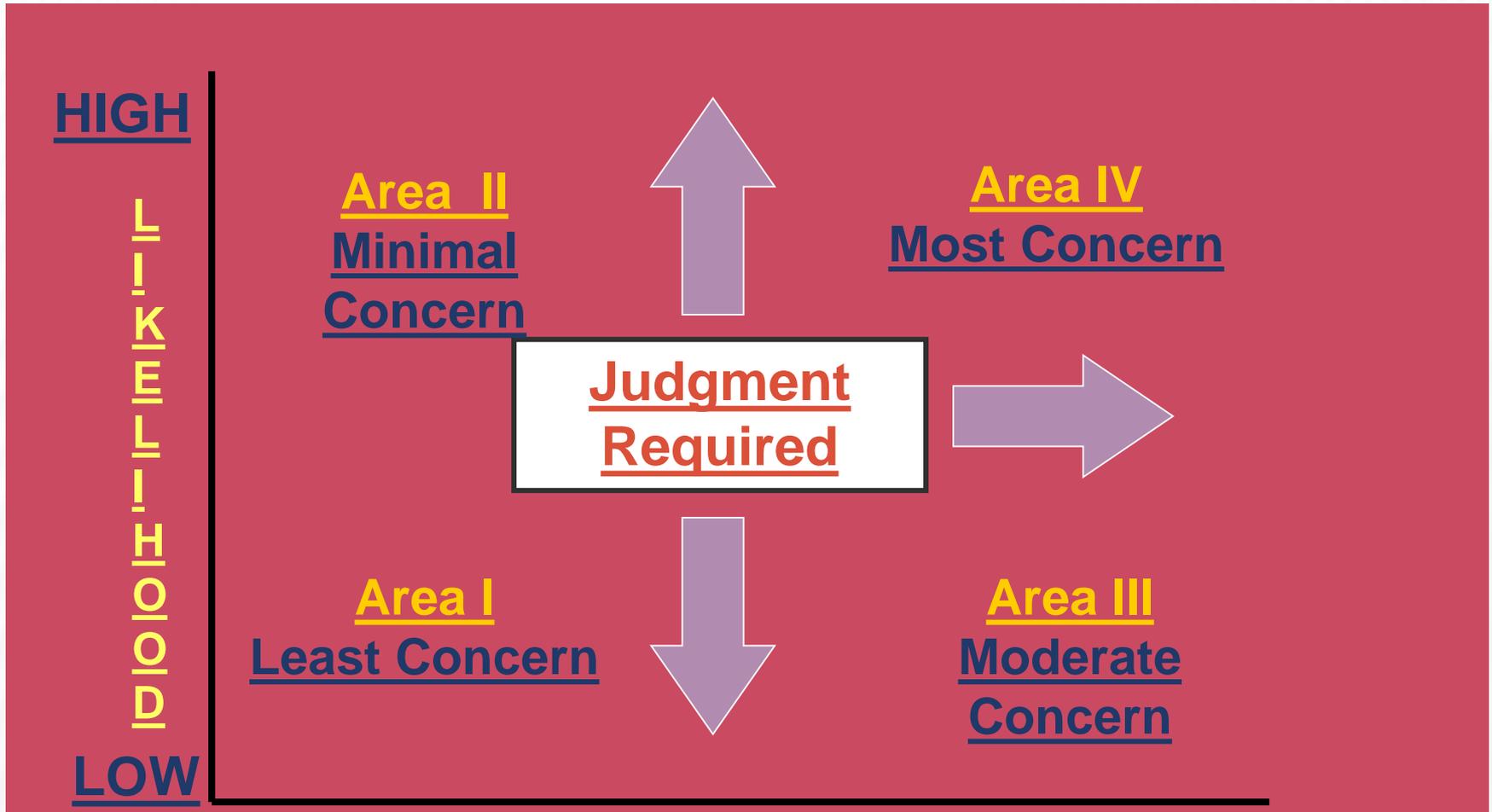


COMMONLY USED CONTROL ACTIVITIES

- Documentation
- Approval and Authorization
- Verification
- Supervision
- Separation of Duties
- Safeguarding Assets



RISK & CONTROLS



LOW

IMPACT

HIGH

COST VERSUS BENEFIT



The cost of the controls shouldn't be greater than the cost of the potential loss



Ensure controls are ...

- Cost effective
- Adequate to manage risk
- Included in system design
- Monitored & periodically evaluated



QUESTIONS?

