

# Risk Assessment 101

Anna Tomassacci, Jaimie Corvetti and Adriana Alfeo



NYS COMPTROLLER

**THOMAS P. DiNAPOLI**

---

# Harvesting Knowledge

2016 Fall Conference | October 25-26

## Office of Operations

John Traylor, Executive Deputy Comptroller

## Division of Contracts & Expenditures

Margaret N. Becker, Deputy Comptroller  
Bernie McHugh, Director, Bureau of State Expenditures



NYS COMPTROLLER  
**THOMAS P. DiNAPOLI**

---

# Objectives

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



# Agenda

- Risk Assessment Preliminary Review Questions
- Internal Controls Overview
- Group Exercise:
  - Perform a Basic Risk Assessment for Accounts Payable Departments
  - Understand the process through interviewing
  - Rank risks in terms of impact and likelihood
  - Design a system of internal controls



# Let's Begin!



NYS COMPTROLLER  
**THOMAS P. DiNAPOLI**

# Preliminary Review

- What is COSO?
  - Committee of Sponsoring Organizations of the Treadway Commission (COSO)
- What are internal controls?
  - Processes that are designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.
- What are the three objectives of internal controls?
  - Operations, Reporting, and Compliance
- What are the five components of internal controls?
  - Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring.
- What is a risk assessment?
  - An evaluation to determine the possibility that an event will occur and adversely affect the achievement of the objectives.



# 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?



# Understand the Process

- Talk to the people actually doing the work
  - Ask where they think there are risks
  - Find out what they actually do
- Do not rely solely on the policies and procedures



# 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:

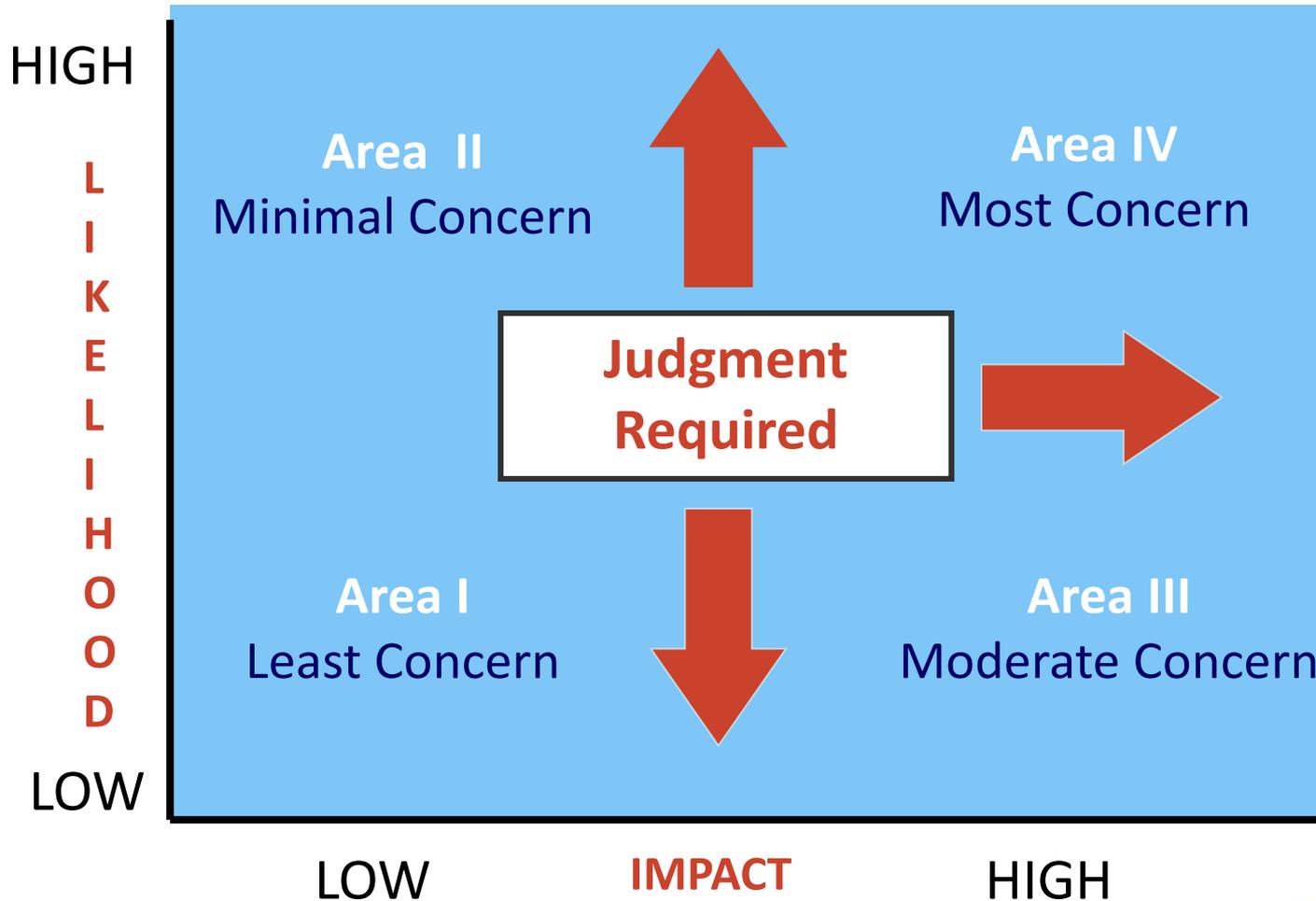
1. no internal controls, or
2. existing internal controls.

## Impact

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

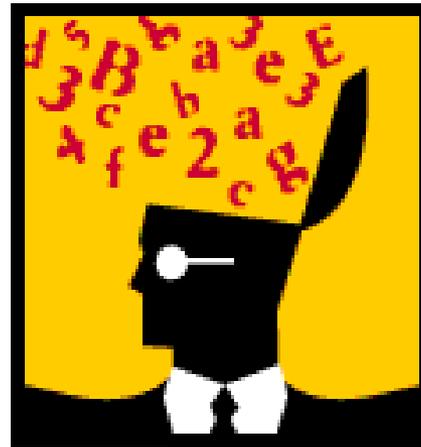


# Evaluating Risk



# Things to Keep In Mind

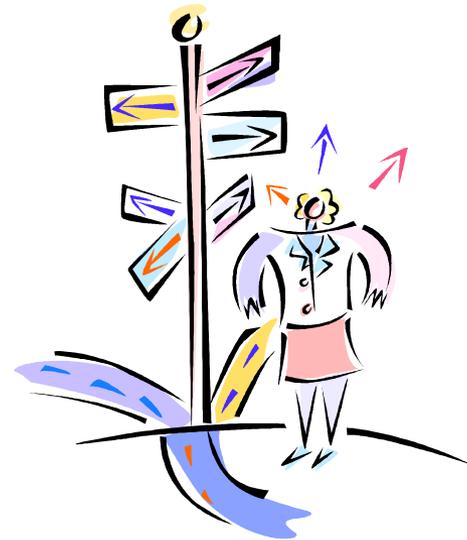
- Change is the one constant
- A risk assessment is never “done”
- Communication and education can make all the difference
- The greatest risk is turning a blind eye to the possibility of risk
- Knowledge is power!



# Managing Risk

## 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.

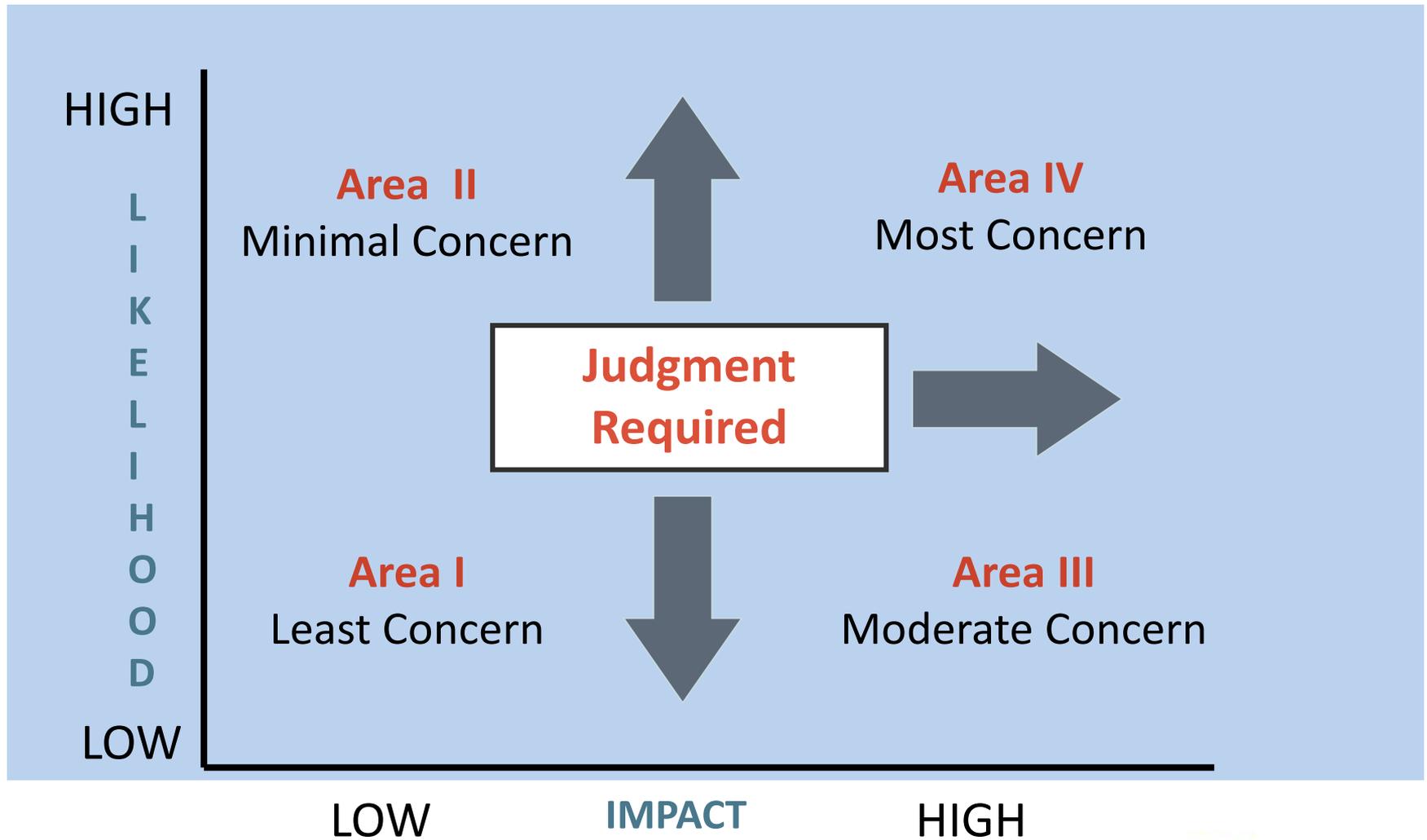


# Commonly Used Control Activities

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



# Risk and Controls



# Cost Versus Benefit



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



# Management's Responsibilities

## Ensure controls are ...

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



# Questions?



# Case Study

## Background

- Agency CLN01 is responsible for all of the cleaning and general maintenance of property owned or leased by the City of Tiny Town. The Agency performs its function by hiring contractors to do the work. The contractors bill the Agency based on time and materials. The City owns and operates 10 buildings and has about 20,000 employees.



# Case Study

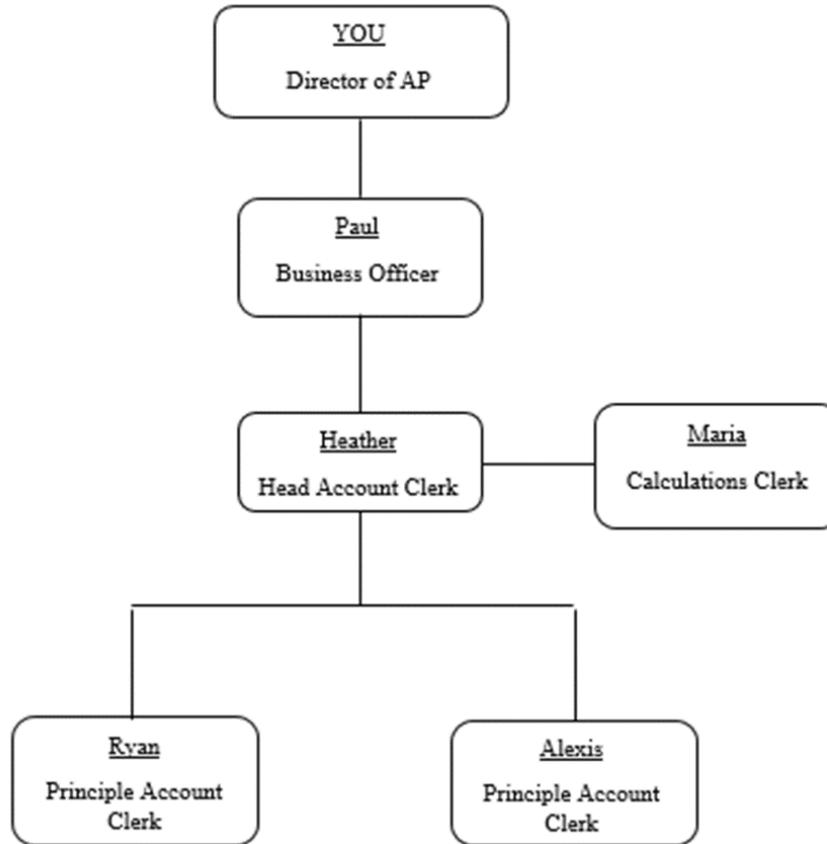
## Background

- You were just hired as the Director of AP. Your first action item is to perform a risk assessment and determine the best use of your resources.
- There are no written policies and procedures
- This is your first day and you have to meet with your boss this afternoon. She would like you to give her your initial assessment at that time.



# Case Study

## Organization Chart



# Case Study

- Identify Operational, Compliance, and Reporting Objectives
- Select one Objective that you will use throughout the Case Study



# Case Study

- Brainstorm about the possible Risks for your one Objective
- Pick what you think are the top three Risks



# Case Study

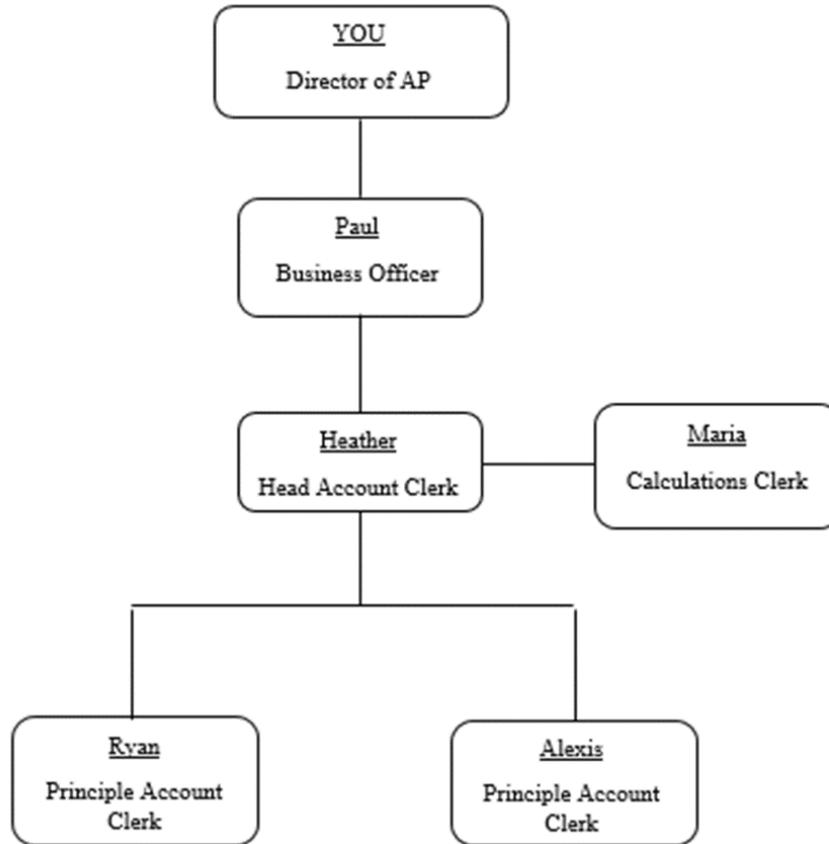
## Interviewing

- Brainstorm about possible questions to ask your staff
- As a group you will have five minutes to ask questions to each staff member



# Case Study

## Organization Chart



# Case Study

- Regroup and see if you have any additional questions to ask your staff
- You will have an opportunity to ask additional questions.



# Case Study

- Identify Control Strengths and Weaknesses as they relate to your objective



# Case Study

## Rank the Risks

- Assign Impact and Likelihood to the Top 3 Risks as if there were no Controls in Place
  - Graph the Risks
- Rank the Risks again taking Control Strengths and Weaknesses into Account
  - Graph the Risks



# Case Study

## System of Controls

- Design sufficient controls to mitigate your risks and address related weaknesses if necessary



# Case Study

Questions?

