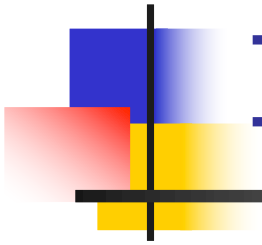


Internal Control Framework

NMASBO

Boot Camp

Take Away Items

- An internal control system is made up of 5 components; Control/organizational environment, risk assessment, control activities, information and communication, and monitoring. Which component is the most important?
- Segregation of duties is part of what component of the internal control system?
- What are the components of the fraud triangle?
- Why is it important to maintain proper segregation of duties?

Session Agenda

- Internal Control Framework
- Risk and Materiality

What are internal controls?

- Internal controls means a process implemented to provide reasonable assurance regarding the achievement of objectives in:
  - Effectiveness and efficiency of **Operations**;
  - Reliability of **reporting**: and
  - **Compliance** with applicable laws and regulations.

Statutory/Regulatory Reference

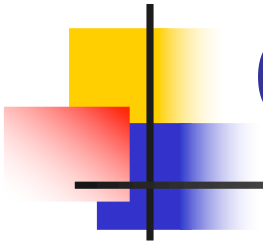
- NMAC 6.20.2.11 INTERNAL CONTROL STRUCTURE STANDARDS:
  - A. Every school district shall establish and maintain an internal control structure to provide management with reasonable assurance that assets are safe-guarded against loss from unauthorized use or disposition, that transactions are executed in accordance with management's authorization and recorded properly to permit the preparation of general purpose financial statements in accordance with GAAP, and that state and federal programs are managed in compliance with applicable laws and regulations. The internal control structure shall include written administrative controls (rules, procedures and practices, and policies that affect the organization) and accounting controls (activity cycles, financial statement captions, accounting applications including computer systems) that are in accordance with GAAP.

Statutory/Regulatory Reference

- MOP PSAB Supplement 2
- "Management is responsible for developing detailed policies, procedures, and practices and ensuring that they are an integral part of the district's operation."

In General

- Internal should -
  - Help rather than hindrance
  - Make sense
  - Part of day to day operations
  - Cost effective
  - Communicated



Components

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

Control/Organizational Environment

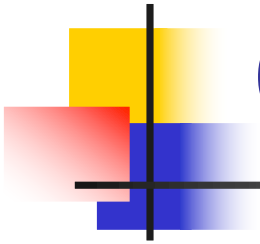
- An entity's control environment represents management's and the board's attitude, awareness, and actions about internal control.
- What is the tone at the top?
- Management must
  - Establish Appropriate control environment
  - Train staff to understand and use appropriate control in all areas.
  - Provide structure and process for implementing these controls.

Risk Assessment

- What could go wrong?
- What assets need protecting?
- A risk is the possibility of an event that threatens an entity's ability to meet its objectives.
- Two types of risk
  - External
  - Internal
- Risk increases during a time of change
- **Management's role is to identify risk areas and manage the risk.**

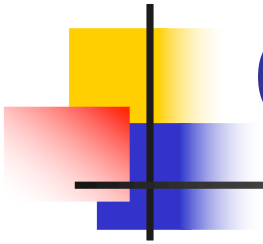
Control Activities

- Established procedures
- Those policies and procedures and the information system that management establishes to provide reasonable assurance that their objectives are achieved.
- Include the design, implementation, and maintenance of policies and procedures.
- **Aim policies and procedures at identified risk**.
- Avoid excessive controls, which are as harmful as excessive risk and result in increased bureaucracy.



Control Activities

- **Preventive** – authorization lists, computer edits, segregation of duties and supervisory approval.
- **Detective** – reconciliation, exception reports, and supervisory review.



Control Activities

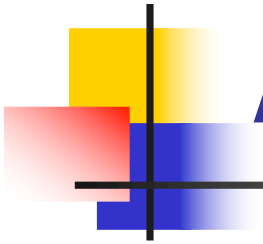
- Are established over
  - Authorization and execution of transactions
  - Segregation of duties
  - Design and use of documents and records
  - Access to assets and records

Segregation of duties

- No policy or procedure can prevent collusion.
- Components of a transaction
  - Authorization - Management
  - Execution - Custodial
  - Recording - Accounting
  - Balancing/checks - Monitoring

Design and Use of Documents and Records

- Aid in recording transactions correctly
- Audit trail
- Forms should be
  - Multiple uses
  - Easy



Access

- Only authorized personnel should have access to assets and records.

Information & Communication

- To operate efficiently, information should be communicated in a form and time frame that enables people to discharge their assigned responsibilities.
- Information must be reliable for effective and timely decision making.

Information & Communication

- Policies and procedures must be communicated to those who need it.
- How do we do this?
  - Written procedural statement
  - Flow charts
  - Web site

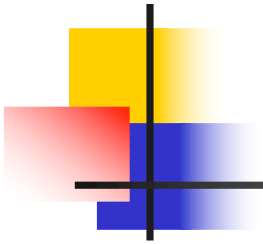
Monitoring

- To assure quality, internal controls should be monitored-through continuing or periodic evaluations, or both – and discrepancies resolved by management at least one level above those responsible.

Analyzing

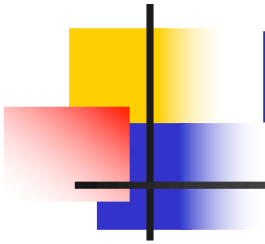
- Internal control policies and procedures are not static.
- Include the design, implementation, and maintenance of policies and procedures.
- Aim policies and procedures at identified risk.
- Avoid excessive controls, which are as harmful as excessive risk and result in increased bureaucracy.
- Ask Why?
- Flow chart current practice
- Review flow chart for unnecessary redundancies.

Risk and Materiality



Risk

- What could go wrong?
- What assets need protecting?
- Possibility of an event that threatens an entity's ability to meet its objectives.
- Risk increases during a time of change
- Management's role is to identify risk areas and manage the risk.
- How do we identify the risk?



Risk

- Availability / Accessibility
- Liquidity
- Visibility (what will get you in the news)

Risk of Fraud

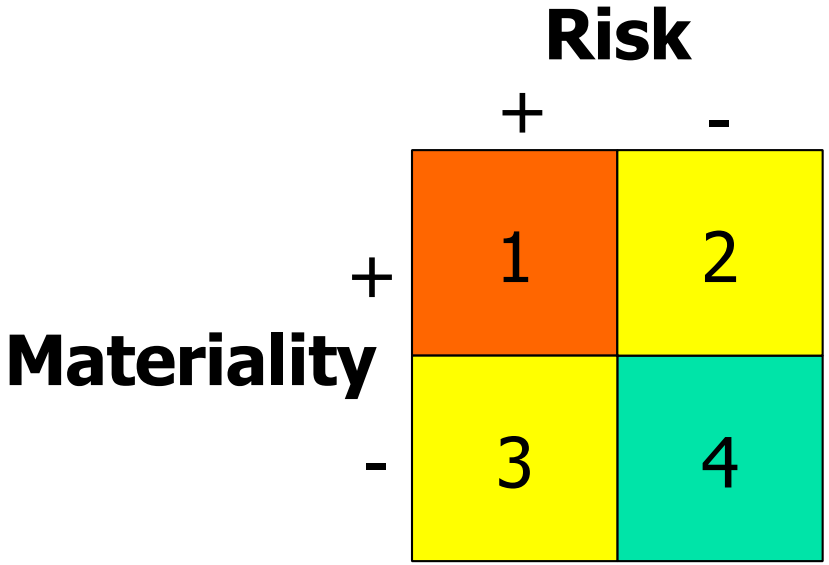
- Auditors are not good at detecting fraud.
- Fraud Triangle
  - Motivation
  - Opportunity
  - Rationalization – highly motivated and seeks opportunity.
    - Frustrate one and you reduce the frequency of fraud.

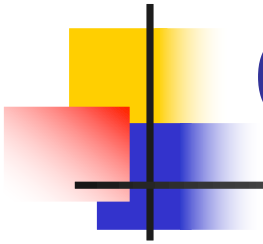
Materiality

- Would this information or data be important to the end user?
- Legal requirements are always material.
- Who are the end users?
  - Superintendent
  - Program admin
  - PED
  - TAXPAYERS

The Threat Matrix

- 1- High risk/ High materiality
- 2 – Low risk/ High materiality
- 3 – High risk/ Low materiality
- 4 – No problem





Closing Remarks

- Questions Comments