Internal Control is Everyone’s Responsibility
What can happen when Internal Control Fails?

- Boeing 737 Airplane Crashes: Software issues; hundreds of fatalities; grounded aircraft
- Fire in Notre Dame Cathedral in Paris
- Theft and Fraud
- Loss of Assets
- Acquisition and Contracting Failures
- PII Compromised
- ADA Violations
- Improper Payments
Consider This...

Major “blowups” do **NOT** come from a single internal control failure, but rather from

the cumulative effect of many small internal control failures.
Overview

- Definition of internal control
- Why we perform internal control
- Federal Managers Financial Integrity Act (FMFIA) requirements
- Control objectives and control activities
- Risk assessment and management
- GAO’s Standards for Internal Control
- Internal control process
- Internal control review and testing
- Classifications of internal control deficiencies
- The corrective action plan (CAP)
- Internal control reporting
CONTROLLING: Classic Management Function, But a Lack of Understanding

Unfortunately, internal control is often improperly perceived as:

- A bean counter, financial, or auditing function
- Too administrative and not operational
- Not critical to mission accomplishment
- Not important to program managers
- A paperwork exercise
Discussion Question

How do we better communicate the importance of internal control?
Accountability – Increasing Focus

- Use of resources is consistent with agency mission
- Programs and resources are protected from waste, fraud, and mismanagement
- Laws and regulations are followed
- Reliable/timely information is obtained, maintained, reported, and used for decision-making
Basic Provisions of the Integrity Act

**Agency Heads**

- Report to the president and Congress annually:
  - A statement of reasonable assurance on controls
  - Any material weakness
- Will report annually on whether financial systems conform to government-side requirements

**GAO**

- Will prescribe internal control standards

**OMB**

- Will issue guidelines for agencies
FMFIA and OMB Circular A-123
Basic Reporting Requirements

Separate statements of assurance required:

• Operational Controls
• Financial Management Systems
GAO’s Definition of Internal Control

An integral component of organization’s management that provides *reasonable assurance* that the following objectives are being achieved:

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

• Federal Managers Financial Integrity Act (FMFIA)

• GAO’s Standards for Internal Control in the Federal Government (Green Book – expanded 2014)

• OMB Circular A-123: Management's Responsibility for Enterprise Risk Management and Internal Control (July 2016)

• DODI 5010.40: Managers’ Internal Control Program Procedures (July 2010)
A-123: Major Changes in July 2016 Issuance

**AGENCIES MUST:**

- Establish an Enterprise Risk Management (ERM) program
- Develop and annually submit risk profiles
- Link ERM planning to strategic objectives
- Assess internal control against the 5 internal control components **AND** the 17 principles
- Put more emphasis on fraud, grant, and ADA risks
Effective Enterprise Risk Management

• Is part of decision-making
• Is based on best available information
• Is transparent and inclusive and
• Facilitates continual improvement of an organization
Terms to Know

- Assessable unit
- Control objective
- Control activity
- Material weakness
- Reasonable assurance
- Risk
- Testing
Define minimum level of quality acceptable for internal control in the government

Provide criteria against which all management systems/controls are to be evaluated

Apply to all aspects of agency’s operations, programs, financial activities, and compliance

Provide a general framework for management to develop detailed policies, procedures, and practices to fit its agency's operations and ensure that they are built into and are an integral part of operations

Emphasize that standards are reflected in and are an integral part of operations
The Five Components of the GAO Internal Control Standards

- **C** Control Activities
- **R** Risk Assessment
- **I** Information and Communication
- **M** Monitoring
- **E** Environment
The Three Major Types of Risk

1. INHERENT
2. PEOPLE
3. CONTROL
# Risk Management Matrix

<table>
<thead>
<tr>
<th>Entity: ________________</th>
<th>Preparer: ________________</th>
<th>Contact Info: ________________</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mission, Goal, Control</strong></td>
<td><strong>Identify Risk(s) — List Separately and Describe</strong></td>
<td><strong>Results of Risk Analysis — Risk Assessment Rating (Use Risk Matrix to Determine)</strong></td>
</tr>
<tr>
<td><strong>Objective, or Process — Identify Which</strong></td>
<td><strong>Control(s) Associated with Risk — Describe All That Apply</strong></td>
<td><strong>Testing — Describe Test Methodology</strong></td>
</tr>
<tr>
<td><strong>Condition of Control after Testing (Effective, Needs Improvement, No Control, or Unnecessary)</strong>&lt;sup&gt;1&lt;/sup&gt;</td>
<td><strong>Status of Corrective Actions for Categories Other Than “Effective”&lt;sup&gt;2&lt;/sup&gt;</strong></td>
<td><strong>Completion Date of Corrective Action, and New Risk Rating</strong></td>
</tr>
<tr>
<td><strong>Office or Unit Responsible and Point of Contact</strong></td>
<td><strong>Level of Deficiency; (A) Control, (B) Significant, or (C) Material Weakness; Highlight Any B or C Type Across Row&lt;sup&gt;3&lt;/sup&gt;</strong></td>
<td></td>
</tr>
</tbody>
</table>

---

<sup>1</sup> Condition of control effective (works as intended and people carrying it out); needs improvement (needs strengthening OR people are not following it; no control in place (needs to be developed); redundant/unnecessary.

<sup>2</sup> A Corrective Action Plan (CAP) should be prepared for each key control needing action. This will allow management to track and report on improvements.

<sup>3</sup> Management should be able to tell at a glance which goal and objectives are affected by control weaknesses.
Risk Assessment Definitions

**RISK**
The chance of something happening that will have a negative impact on objectives. It is measured in terms of likelihood and consequences.

**LIKELIHOOD**
A qualitative description of a probability or frequency.

**CONSEQUENCE**
The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage, or gain.
Risk Heat Map

Risk score = C x L

CONSEQUENCE

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>5</td>
<td>10</td>
<td>15</td>
<td>20</td>
<td>25</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
<td>20</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>15</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>10</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

LIKELIHOOD
Categories of Control Activities

- Top-level reviews of actual performance
- Reviews by management at functional or activity level
- Management of human capital
- Controls over information processing
- Physical control over vulnerable assets
- Establishment and review of performance measures and indicators
- Segregation of duties
- Proper execution of transactions and events
- Accurate and timely recording of transactions and events
- Access restrictions to and accountability for resources and records
- Appropriate documentation of transactions and internal control
Quiz:
How Do We Achieve Quality?

☐ A. Working harder

☐ B. Getting more resources

☐ C. Through well-designed processes that allow us to efficiently deliver products that effectively accomplish mission and satisfy customers

☐ D. Having more fun on the job
Overview of Internal Control Process

1. Organize the process
2. Conduct risk assessments
3. Conduct internal control reviews
4. Track internal control and corrective action plans

- Segment the agency
- Develop management control plans and update annually
- Take corrective actions
- Prepare reports on results
Detail of Internal Control Process

Organize the Process
- Assign Responsibilities
- Develop Tracking System
- Maintain Proper Records
- Commit Adequate Staff and Resources
- Develop and Conduct Training

Conduct Risk Assessments
- Identify and Assess Risks
- Assign Risk Rating

Develop Control Plan
- Establish or Refine Monitoring Procedures
- Modify Manuals and Instructions
- Schedule Reviews

Conduct Internal Control Reviews
- Identify and Select Event Cycles and Processes
- Identify Control Objectives and Techniques
- Test Control Objectives and Techniques
- Recommend Corrective Actions
- Use Alternative Control Reviews

Implement Corrective Actions
- Identify Material Weakness
- Identify Corrective Actions for All Weaknesses
- Select Corrective Actions
- Identify Resources for Corrective Actions

Monitor and Track Weaknesses
- Obtain Closure on Weaknesses

Report on Internal Controls
- Report for Division and/or Branch Management
- Report to Head of Agency
- FMFIA Report to President

Segment the Organization
- Divide Into Assessable Units
Purpose of Internal Control Review (ICR)

An ICR allows management to determine if:

- Positive and supportive control environment exists
- Laws, regulations, and other directives such as policies and procedures are being implemented as directed
- Material weaknesses are indicated
- Controls exist and are cost-effective
- Corrective actions are needed
- Agency might be vulnerable in areas covered by the ICR
MICP Process/Review Steps – DoDI 5010.40

**STEP 1**
Identify areas to be reviewed along with any associated risks

**STEP 2**
Plan and carry out specific ICRs on key areas and risks – TEST

**STEP 3**
Determine the condition of controls; report deficiencies
Internal Control Testing Methods

- Document analysis
- Interviewing
- Observation
- Surveys/questionnaires
- Transaction testing
Classifications of Internal Control Deficiencies

- Control deficiency
- Significant Deficiency
- Material weakness

Controls may have either a design or operational deficiency or both.
Some Factors for Determining What Constitutes a Material Weakness

1. Impacts operating effectiveness of Entity-Level controls
2. Impairs fulfillment of essential operations or mission
3. Deprives public of needed services
4. Significantly weakens established safeguards against fraud, waste, loss, unauthorized use or misappropriation of funds, property, other assets, or conflicts of interest.
# Commander’s Status Report on Mission Elements Affected by Internal Control Deficiencies

<table>
<thead>
<tr>
<th>Key Mission Element</th>
<th>Internal Control Deficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Equipment readiness</td>
<td>1. Insufficient inventory of critical item: <em>Material Weakness</em></td>
</tr>
<tr>
<td>2. Logistics training</td>
<td>2. Required course for 2 logicians not completed: <em>Control Deficiency</em></td>
</tr>
<tr>
<td>3. Backlog of vehicle repairs</td>
<td>3. 35% scheduled maintenance overdue: <em>Reportable Condition</em></td>
</tr>
</tbody>
</table>
DoD Reported Material Weaknesses

For 2018, DoD reported in its Agency Financial Report (AFR) 58 material weaknesses.

38 in internal control over financial reporting (ICOFR); e.g., in areas of Fund Balance With Treasury, military pay, civilian pay, real property

20 in non-financial operations; e.g., in areas of resource management, force readiness, supply operations

3 in non-compliances associated with financial systems.
Correcting Material Weaknesses

- Take timely action
- Set milestones with completion dates
- Periodically assess progress
- Follow up
DoD Levels of Material Weaknesses

**COMPONENT LEVEL**

- Merits OSD attention or exists in a majority of components
- Those not resolved at the SECDEF level are reported in the annual Statement of Assurance

**DOD LEVEL**

- Permeates a component or one or more of its major commands or activities
- Requires component head attention

**MAJOR COMMAND OR FIELD ACTIVITY LEVEL**

- Permeates a major command or one or more of its installations/activities

**INSTALLATION OR ACTIVITY LEVEL**

- Requires the attention of the head of an installation
Reporting Levels in DoD

- Office of the Secretary of Defense
- Military departments
- Joint Chiefs of Staff
- Combatant commands
- Office of the Inspector General
- Defense agencies
- Field activities
- Other organizational entities
Statement of Assurance

- Represents agency head’s informed judgment as to overall adequacy and effectiveness of internal controls within the agency

- Must take one of the following forms:
  - Statement of Assurance:
    - Unmodified
    - Modified
  - Statement of no assurance

- What form did DoD’s assessments take in 2018?
What Are We Assuring?

- Operations are effective, efficient, and meet objectives
- Financial and performance reporting are reliable and timely
- Agency complies with laws and regulations
- Programs are managed with integrity and follow high ethical standards
- Agency is protecting its assets
- Agency's approach considers five components of internal control
Sources of Information

- Leadership knowledge gained from daily operations of DOD
- Reviews conducted for purpose of assessing Internal Control
- OIG and GAO reports
- Program Evaluations
- Audits of financial statements
- Reviews of financial systems under OMB circular A-123, App D
- Annual performance plans and reports pursuant to GPRAMA
- Annual reviews and reports under IPIA, IPERA, and IPERIA
- Other financial and performance audit reports
- Other reviews relating to DOD operations

*Components will consider deficiencies from all sources, **BUT primarily** from component’s **own testing** (DoDI 5010.40)*
Benefits of Internal Control

- Provides management with added confidence regarding achievement of objectives
- Provides feedback on how effectively component is operating
- Helps reduce risks related to achieving components objectives
- Safeguarding of assets
See you in Nashville in 2020
THANK YOU!

Follow us on Twitter @ Mgmt_Concepts

www.MangementConcepts.com