Agency Risk Management & Internal Control Standards (ARMICS)
Emphasis on Internal Controls

- The Sarbanes-Oxley Act of 2002
- Statement of Auditing Standards (SAS) 112: Communicating Internal Control Related Matters Identified in an Audit - lowers the bar on internal control weaknesses reported by auditors
- Commonwealth of Virginia Comptroller has mandated internal control assessments at agencies and institutions – Agency Risk Management and Internal Controls Standards (ARMICS)
Commonwealth’s Vision Statement

“We have a responsibility to be the best-managed state in the country. To do so, we must have a focused vision, and a fiscally responsible system that provides clear, measurable objectives, outcomes and accountability, and that attracts, motivates, rewards, and retains an outstanding state workforce.”
Agency Risk Management and Internal Control Standards

Internal Control Concepts
Internal Control

“Internal control is an ongoing process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effective and efficient operations
- Reliable financial reporting
- Compliance with laws and regulations
- Safeguarding assets
Responsibility for Internal Control?

- Governing Boards
- Executive Management (Agency Heads)
- Senior and Line Management (including CFOs and Fiscal Officers)
- Supervisors and Staff

EVERYONE IS RESPONSIBLE!
Is it only financial statements?

Financial Reporting Disclosures

- Reporting Transparency
- Management Behavior and Accountability
- Internal Control

Photo by Ralph Clevenger
Photo Copyright © 2004, Successories, LLC. All Rights Reserved.
Related Concepts

- Internal control is a **process**. It is a means to an end, not an end in itself.

- People provide internal control. It’s not just policy manuals and forms, but **people at every level**.

- Internal control gives only **reasonable assurance**, **not** absolute assurance.
Internal Control Model

- Control Environment
- Risk Assessment
- Control Activities
- Information & Communication
- Monitoring
Internal Control Model

- Control Environment
- Risk Assessment
- Control Activities
- Information & Communication
- Monitoring
Control Environment

The foundation on which everything rests:

- The “tone” of the agency
- Management’s philosophy
- Integrity and ethics
- Commitment to competence
- Accountability
- Policies and procedures

How would others rate your agency?
The Tone at the Top

- Organization culture
- Agency head leadership
- Communication and full understanding
Internal Control Model

- Monitoring
- Information & Communication
- Control Activities
- Risk Assessment
- Control Environment
Organizational Risk

- Major considerations
  - Risk types
  - Risk considerations
  - Risk mitigation

- Major risks
  1. Financial
  2. Legal Liability
  3. Regulatory Compliance
  4. Organizational Image
  5. Organization-Specific
  6. Data Integrity and Reliability
  7. Confidentiality of Data
  8. Safeguarding Proprietary Data
  9. Contingency Planning
  10. Operations
Purpose of Risk Assessment

Risk assessment enables an institution to consider the extent to which potential events could affect the achievement of objectives.

An “event” is anything that prevents us from achieving an objective as planned, whether that is a “good” event or “bad” event.
Assessing and Managing Risk

Key considerations:

- Event impact
- Event likelihood
- Residual risk
- Risk acceptance
**Internal Control Activities**

- **Control Environment**
  - Monitoring
  - Information & Communication
  - Control Activities
  - Risk Assessment

- **Control Activities**
  - Separation of duties
  - Training and supervision
  - Authorization and approval
  - Review and reconciliation
  - Physical security over facilities, assets, personnel, paper documents, and electronic data
  - Security over confidential records
  - Documentation of policies, procedures, and control activities
Control Activities

- Clearly convey control responsibilities to employees. Ensure they understand.
- Hold employees personally accountable for assigned control activities.
- Do not tolerate management override of controls.
- Make policies and procedures exceptions only when appropriate. Document exceptions thoroughly.
Information and Communication

- Top down
- Bottom up
- Across functional areas
- Everyone on the same page
Information and Communication

- Information is of high quality – useful, timely, relevant, accurate, user-friendly.

- Employee duties and control responsibilities are clearly communicated to them.

- Information systems plans are consistent with administration and agency objectives and plans. Users are effectively involved in systems development.
Information and Communication

- Management is receptive to employee concerns, suggestions, and complaints.
- Communication across the organization and external customers is open and effective.
- Agency standards for business conduct are conveyed to external parties.
- Customer complaints go to the right level and get resolved appropriately.
Internal Control Model

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

- Hold management and supervisors accountable for monitoring staff.
- Hold staff accountable for monitoring their own activities.
- Monitor both hard controls and the control environment.
- Watch for behavioral “red flags.”
- Conduct independent control assessments.
Risk Management Approach and Tools
Evaluating Internal Controls

- Meaningful evaluation of internal controls is the key to reducing the possibility of fraud, waste, and abuse.
- Management must use due diligence.
- Management must document control activities and its evaluation.
Characteristics of Good Internal Controls

- Institutional commitment to integrity and ethics
- Management’s commitment to professional and technical competence
- Organizational structure appropriate to carry out the missions
- Clear assignment of authority and responsibility
- Evaluation of risks
- Effective information and communication systems
- Comprehensive policies and procedures
- Continual monitoring
“Hard Controls”

Often things you can see and touch:
- Required employee signoffs
- Training verification forms
- Document approval by signature, prior to action
- Dual signatures on checks
- Access logs
- Documents matched prior to payment
“Soft Controls”

Sometime less direct than hard controls:

- Compliance incentives
- Standards for hiring and promotion
- Employee compliance training
- Encouraging new ideas
- Periodic employee feedback, interviews
- Customer and supplier feedback
- Management’s reaction to bad news
# Hard Control vs. Soft Control

<table>
<thead>
<tr>
<th>Control Environment</th>
<th>Hard Control</th>
<th>Soft Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>A code of ethics exists</td>
<td>Management acts ethically</td>
<td></td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>A strategic plan is prepared</td>
<td>Employees are familiar w/plan</td>
</tr>
<tr>
<td>Control Activities</td>
<td>A signatories list exists</td>
<td>Employees know signatory limits</td>
</tr>
</tbody>
</table>
# Hard Control vs. Soft Control

<table>
<thead>
<tr>
<th></th>
<th>Hard Control</th>
<th>Soft Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>**Information &amp;</td>
<td>Exception reports are run and sent to</td>
<td>Exception reports are reviewed,</td>
</tr>
<tr>
<td>Communication**</td>
<td>management</td>
<td>understood, and investigated</td>
</tr>
<tr>
<td><strong>Monitoring</strong></td>
<td>Subsidiary records are reconciled to</td>
<td>Employees make suggestions on</td>
</tr>
<tr>
<td></td>
<td>general ledger</td>
<td>better ways to do things</td>
</tr>
</tbody>
</table>
If Deficiencies Are Identified

- Deficiencies must be reported to senior administration.

- Corrective action plan must submitted to include:
  - Description of deficiency and when identified
  - Target date for completion of corrective action
  - Personnel responsible for monitoring progress
  - Indicators/statistics used to monitor progress
  - Target to indicate deficiency corrected

- DOA and APA are expected to review our documentation.
Questions?

Contact:

Angela M. Davis, MBA, CFE
ARMICS/Internal Control Coordinator
804-827-1630
amdavis2@vcu.edu

Feel free to contact me with any questions or concerns.