



Agency Risk Management & Internal Control Standards (ARMICS)

ARMICS and Related Topics

- The Sarbanes-Oxley Act of 2002
- About “internal control”
- Workplace ethics
- Understanding “risk”
- Some risk assessment mechanics
- Tying ARMICS to DPB strategic planning



The Sarbanes-Oxley Act

What is SOX?

“An act to protect investors by improving the accuracy and reliability of corporate disclosures required by securities laws, and for other purposes.”

Why SOX? Scandals, including:

- **WorldCom** – Bernie Ebbers (CEO, 63), 25 years prison – \$11 billion lost
- **Dynegy** – Jamie Olis (VP Finance, CPA, attorney, 38), 24+ years prison – \$105 million lost by 13,000 members in UC Retirement Plan alone
- **Adelphia** – John Rigas (founder, 80) 15 years prison, Timothy Rigas (CFO, 48) 20 years – \$100 million stolen
- **Tyco** – Dennis Kozlowski (CEO, 58) and Mark Swartz (CFO, 44) convicted – 8-1/3 to 25 years prison – pair must pay \$134 million in restitution, \$105 million in fines – “looted” Tyco for \$547 million (NY state courts)
- **Enron** – Ken Lay (CEO, 63) – 4,000 lost jobs & pensions, creditors lost \$65 billion – trial set for January 2006

Scandals? So what?

Like hundreds of pension funds throughout the country, VRS has suffered losses from investments in Enron and WorldCom ... VRS provides benefits to more than 104,000 retirees and has 310,000 active members.

Virginian-Pilot (August 22, 2002)

VRS losses?

- **WorldCom \approx \$50 million.**
- **Enron \approx \$60 million.**

“Those losses represent only a sliver of the billions in value erased from VRS by the two-year decline in the stock market.”

Jeff Shapiro, Richmond Times-Dispatch (July 3, 2002)

Is it only financial statements?

Financial Reporting Disclosures

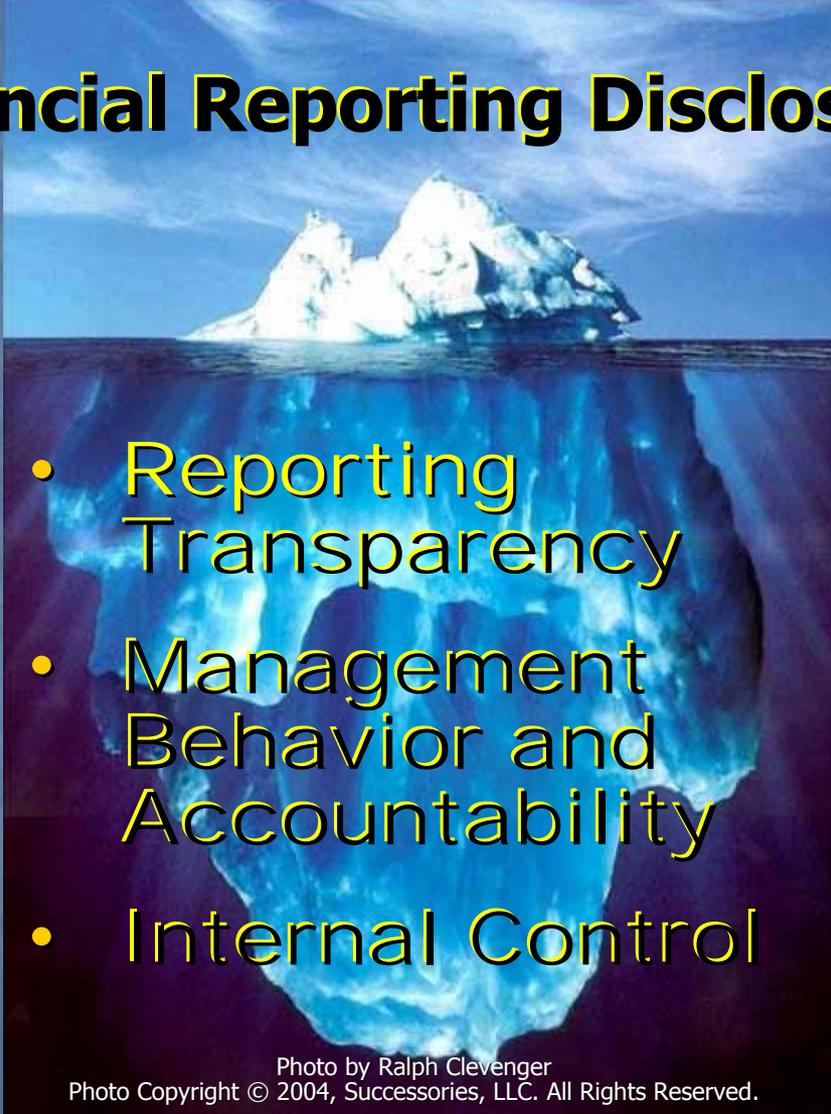
- 
- Reporting Transparency
 - Management Behavior and Accountability
 - Internal Control

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

Key SOX Provisions

- Management must assess internal controls
- CEO, CFO, and the Chief Accounting Officer (CAO \approx fiscal officer) must abide by a code of ethics.
- CEOs and CFOs must certify accuracy of financial statements.
- Must issue annual reports - 60 days.
- CEO and CFO must certify internal controls review 90 days prior to report.
- SOX gives whistleblower protection to employees.

Key SOX Provisions & Sanctions

- Management must assess internal controls
- CEO, CFO, CAO (\approx fiscal officer) must abide by a code of ethics.
- CEOs and CFOs must certify accuracy of financial statements
- Must issue annual reports - 60 days.
- CEO and CFO must certify internal controls review 90 days prior to report.
- Whistleblower protection to employees.
- Higher criminal and civil sanctions: Prison terms \leq 25 years. Fines \leq \$500,000.
- \leq 10 years prison for destroying, altering, concealing, or falsifying records with intent to obstruct or influence an investigation.
- \leq 10 years prison for auditor failure to keep audit work papers for 5 years.
- \leq 10 years for failure to certify financial reports when reports do not comply.
- \leq 20 years for certifying financial statements while knowing they do not comply.
- \leq 20 years prison for tampering with records or impeding an official proceeding.
- Extended statute of limitations (5 years).
- Fines cannot be discharged in bankruptcy.

Does SOX Apply to States?

- Not yet.
- Circular A-123 was revised Dec 2004 to mandate SOX-like standards for Federal agencies.
- The Federal government is expected to apply A-123 to states in the future.
- SOX and ARMICS address parallel issues, and both stem from COSO standards.

SOX Ethics Considerations

- Honesty
- Professional integrity
- Ethical relationships
- Observing all laws & regulations
- Minding appearances and instincts (Would it “pass the smell test?”)

Government Accountability Issues

- Upholding public vs. personal interests
- Recognizing the difference between the floor (e.g., laws, regulations) and the ceiling (e.g., principles, values)
- Doing what is right vs. what is acceptable
- Minding economic substance vs. legal form
- Being concerned with both fact and appearance (e.g., independence)
- Using judgment vs. completing checklists
- Recognizing that continuing improvement in today's rapidly changing world is essential
- Knowing that trust is hard to earn, but easy to lose

David M. Walker, U. S. Comptroller General, May 2, 2005

Internal Control Concepts



What is **COSO**?

Committee **O**f **S**ponsoring **O**rganizations of the Treadway Commission (formed in 1985)



The Institute of Internal Auditors



COSO Defines 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 in the following categories:

- Effective and efficient operations
- Reliable financial reporting
- Compliance with laws and regulations”

A number of writers add “safeguarding assets”

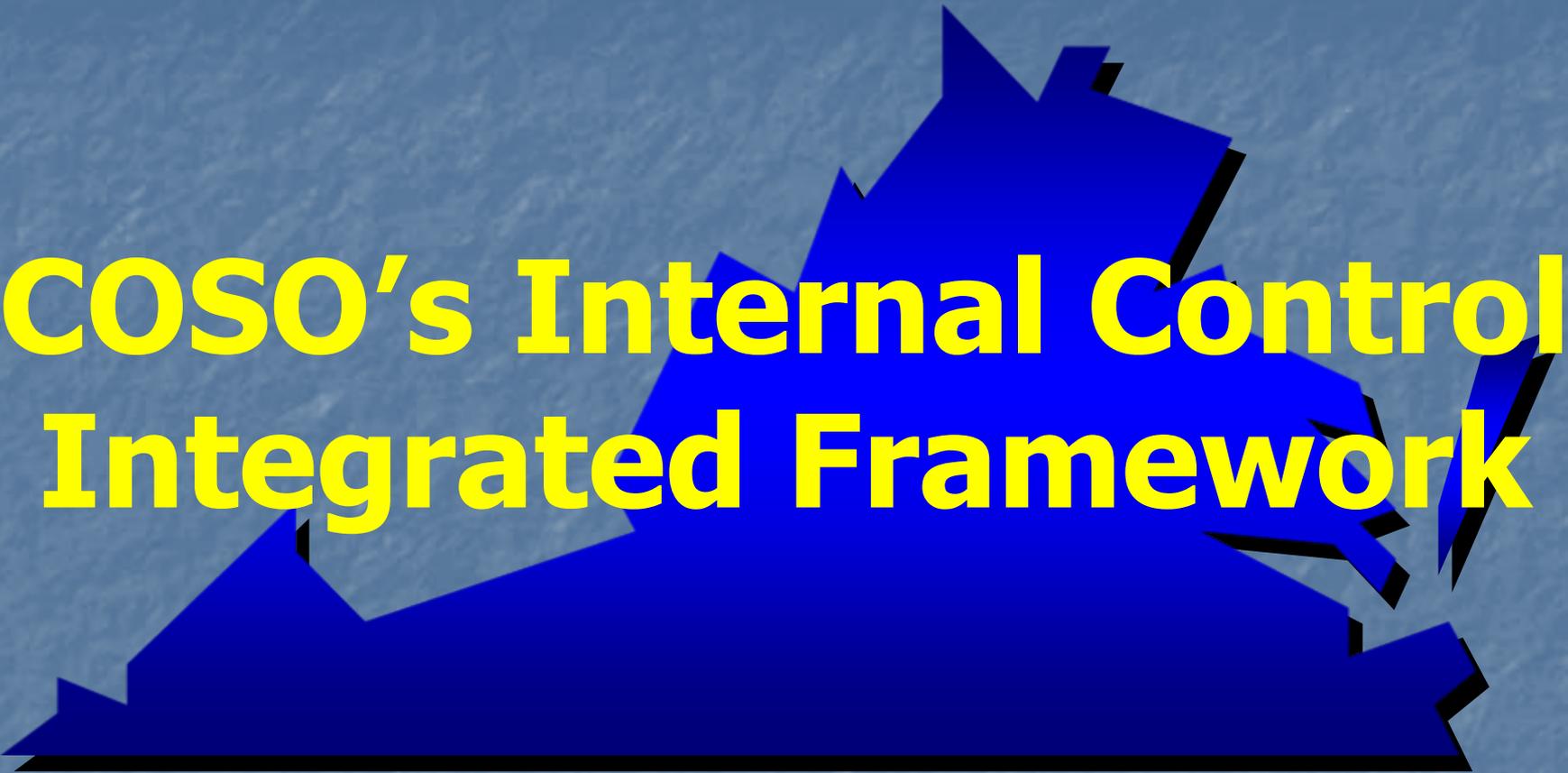
Responsibility for Internal Control?

- Governing Boards
- Executive Management (Agency Heads)
- Senior and Line Management (including CFOs and Fiscal Officers)
- Supervisors and Staff
- **EVERYONE IS RESPONSIBLE!**

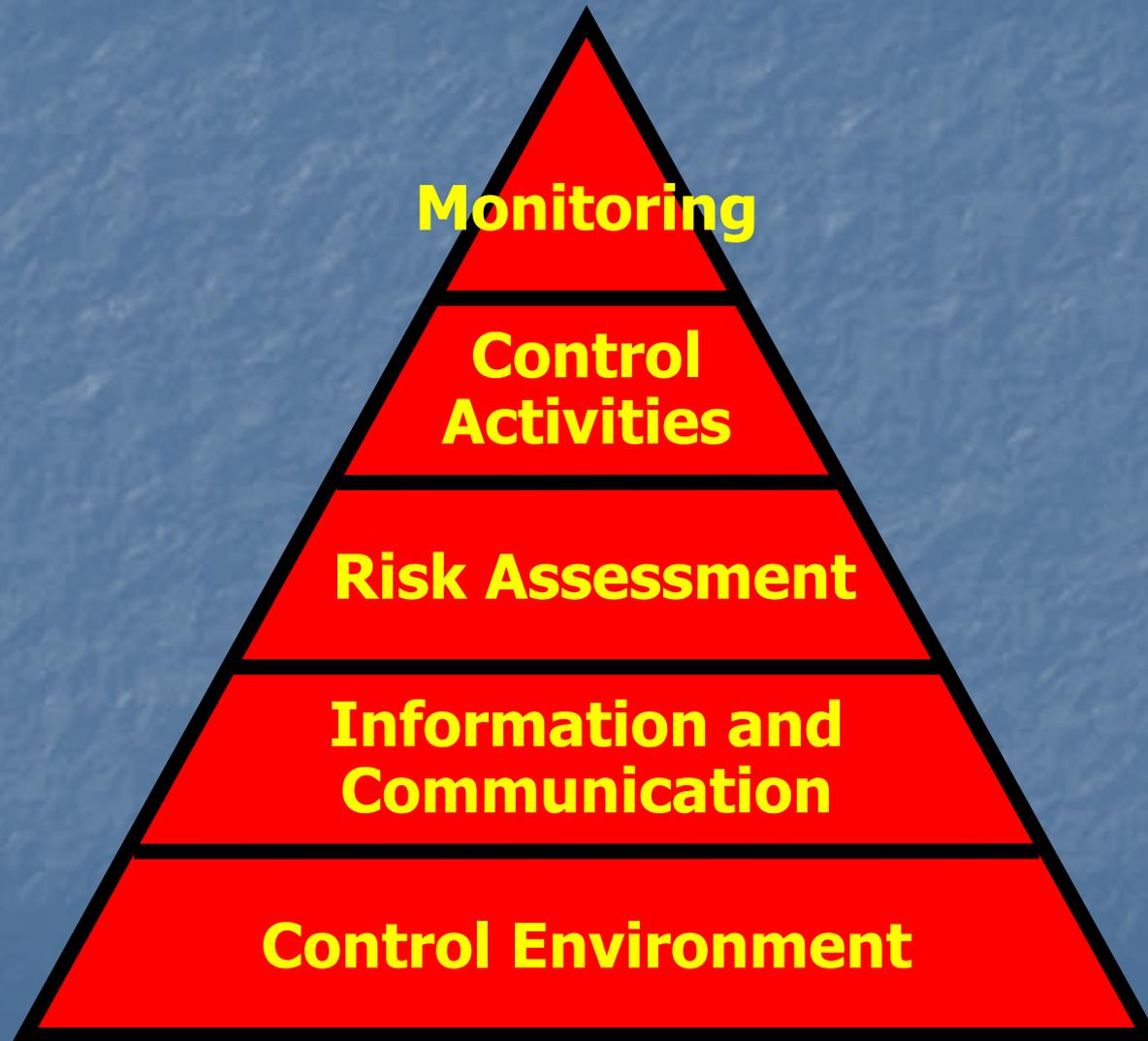
Related Concepts

- 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**.

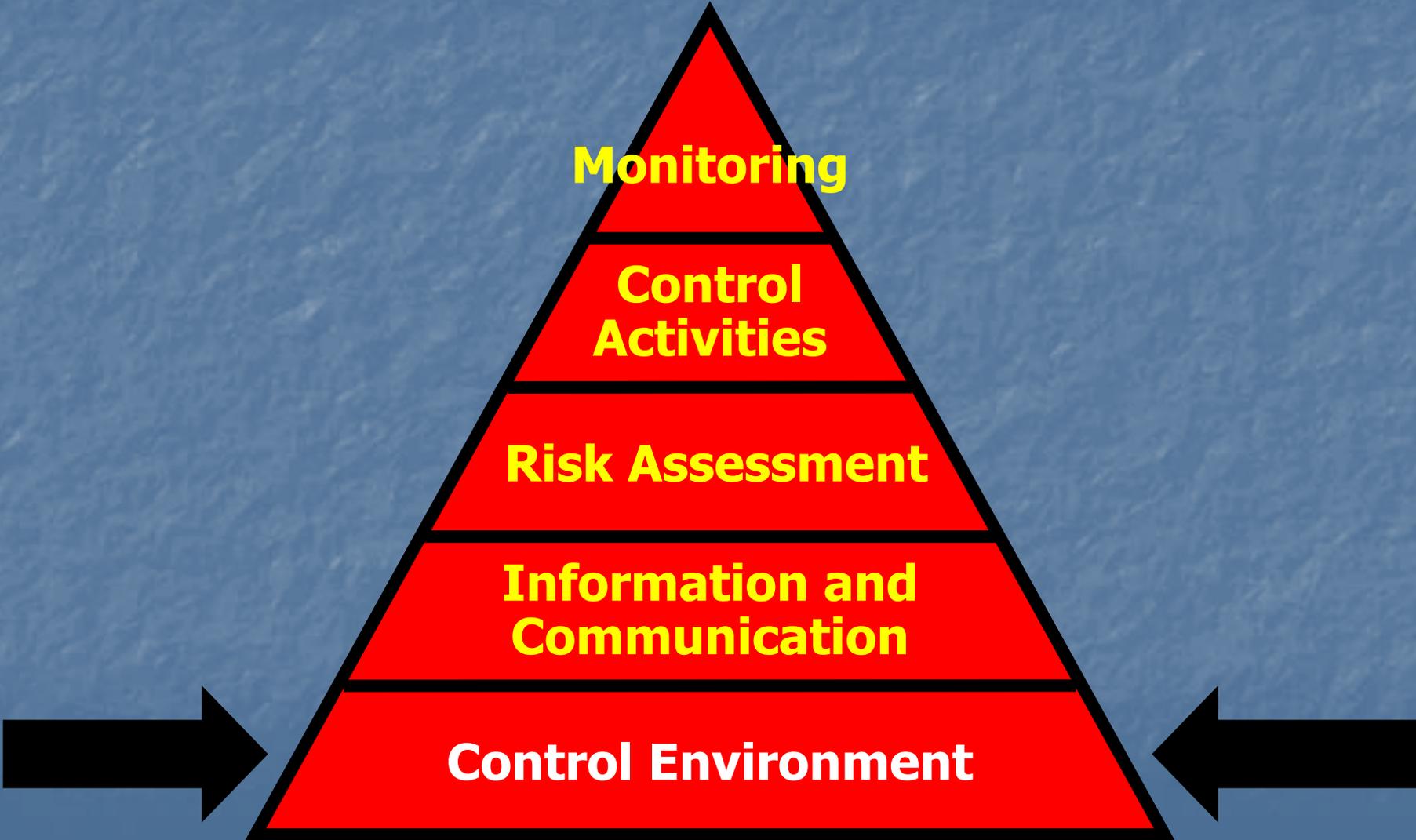
COSO's Internal Control Integrated Framework



First COSO Internal Control Model



First COSO Internal Control Model



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

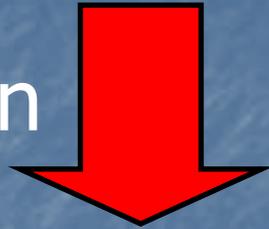


First COSO Internal Control Model

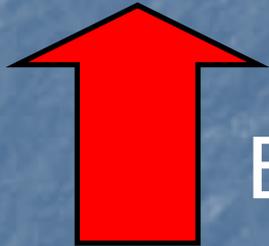


Information and Communication

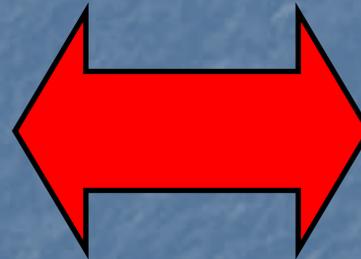
- Top down



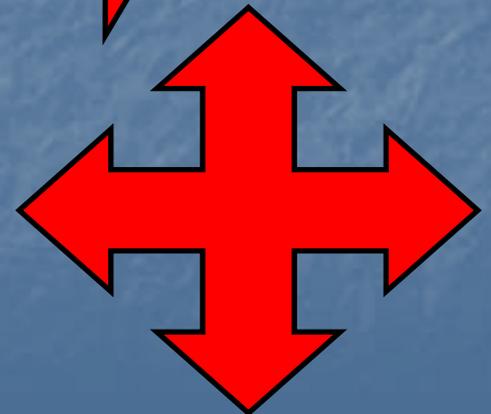
- Bottom up



- Across functional areas



- Everyone on the same page



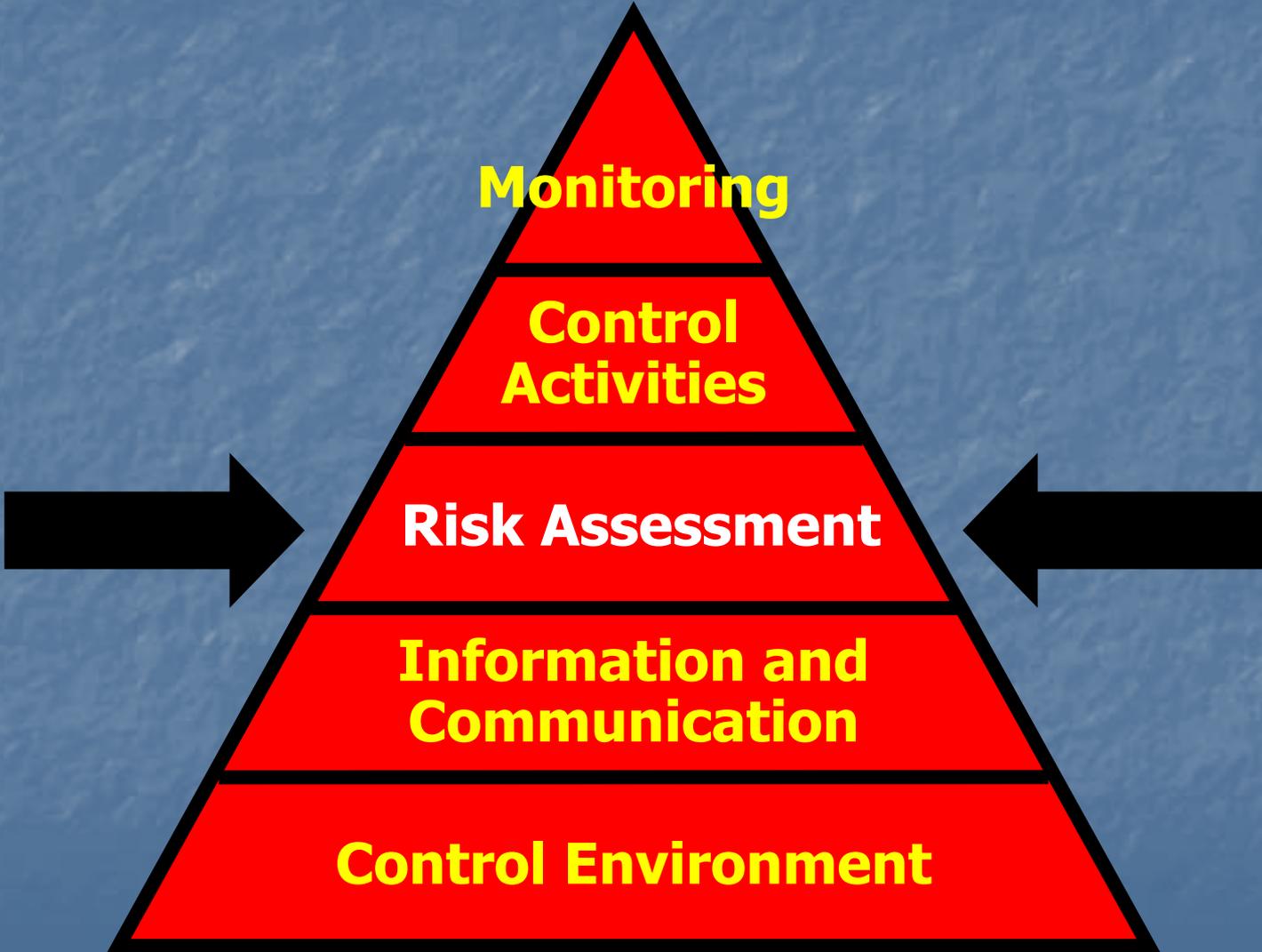
Information and Communication

- 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.

First COSO Internal Control Model



Organizational Risk

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

10 Critical Organizational 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

Organization Risks: Example 1

- VITA requires agencies and institutions to prepare and test a “COOP” (continuation of operations plan) for IT-based systems. A COOP is a type of contingency plan.
- What about the non-technical aspects of programs?
- Does IT contingency planning cover all major risks?

Organizational Risks: Example 2

Governing Magazine (2/05) spies “a **personnel tornado** on the horizon.”

- In most states, 1 in 5 employees will retire in next 5 years. In Tennessee, $\approx 40\%$!
- “We call it the brain drain,” says director of Nevada’s social services department. “I have 9 major divisions ... the head of all but 1 division could leave tomorrow.”

Purpose of Risk Assessment

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

Purpose of Risk Assessment

Remember, 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

Assessing and Managing Risk

Agencies should manage risk to anticipate and handle things that do not go as planned. Ideally, we should plan for both positive and negative events.

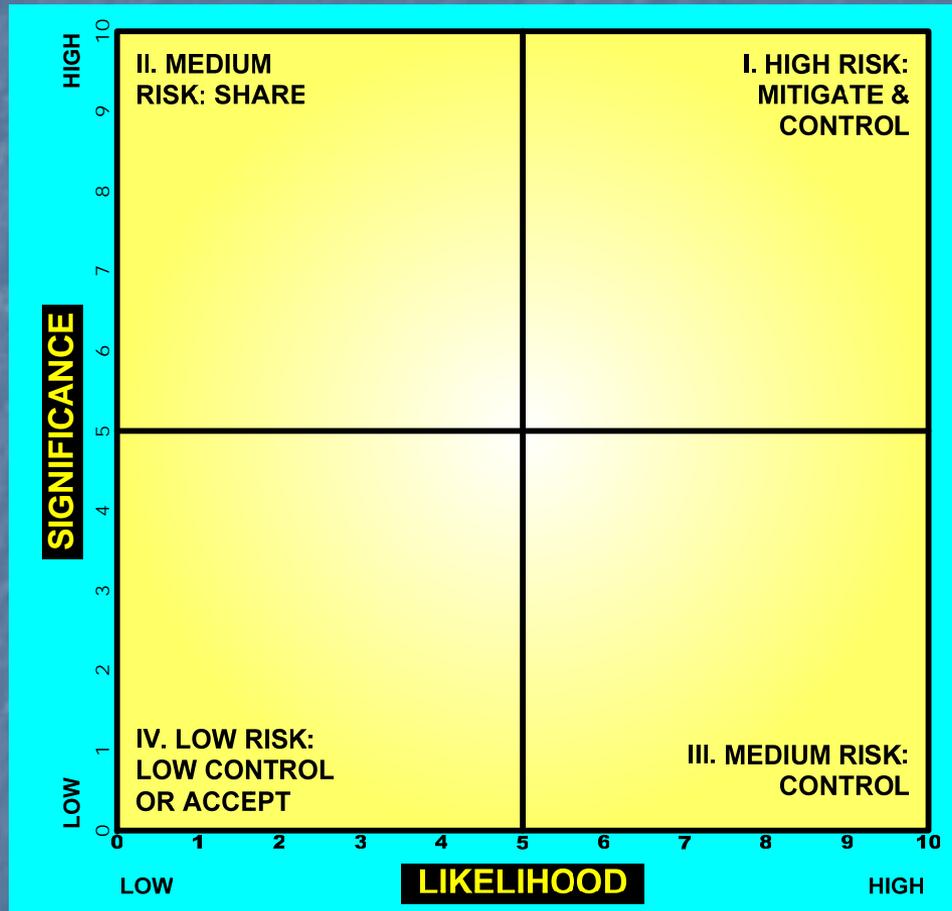
However, governments must first prevent negative events, as reflected in the following slides.

Just remember, risk assessment ideally covers both positive and negative events.

Assessing and Managing Risk

- **Impact** – if a risk event occurs, how bad will it be? Can we estimate how bad?
- **Likelihood** – what are “the odds” that it will happen? Can we estimate the odds?
- How can we compare risk events based on both potential impact and likelihood? One technique is creating a “**risk map.**” The next 2 slides illustrate risk mapping.

A Sample Risk Map

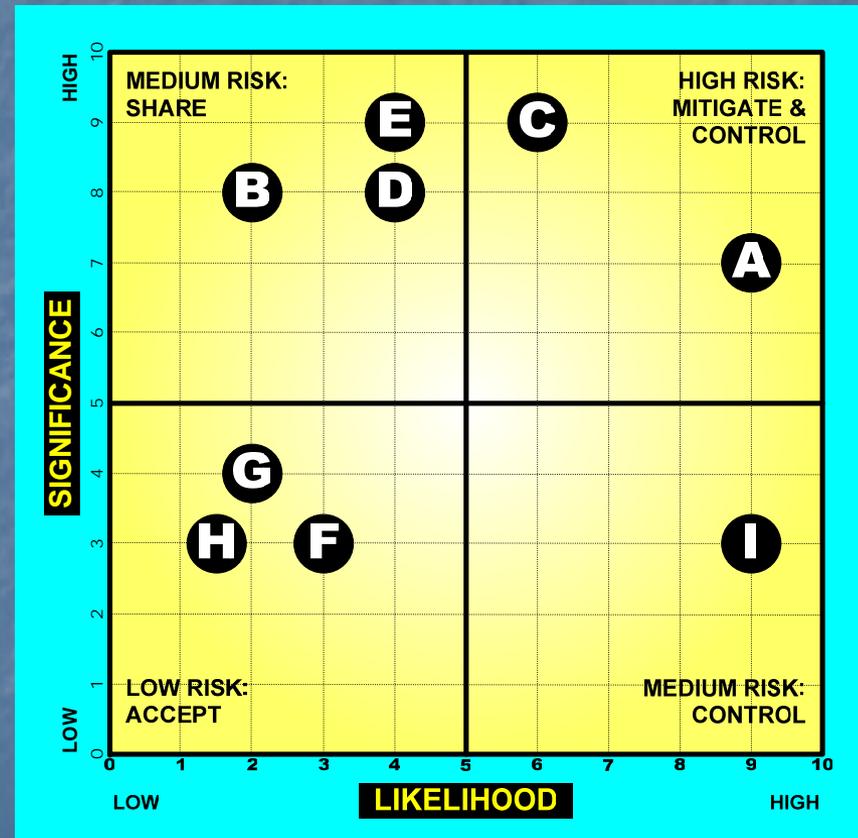


Mapping Risks for an IT Help Desk

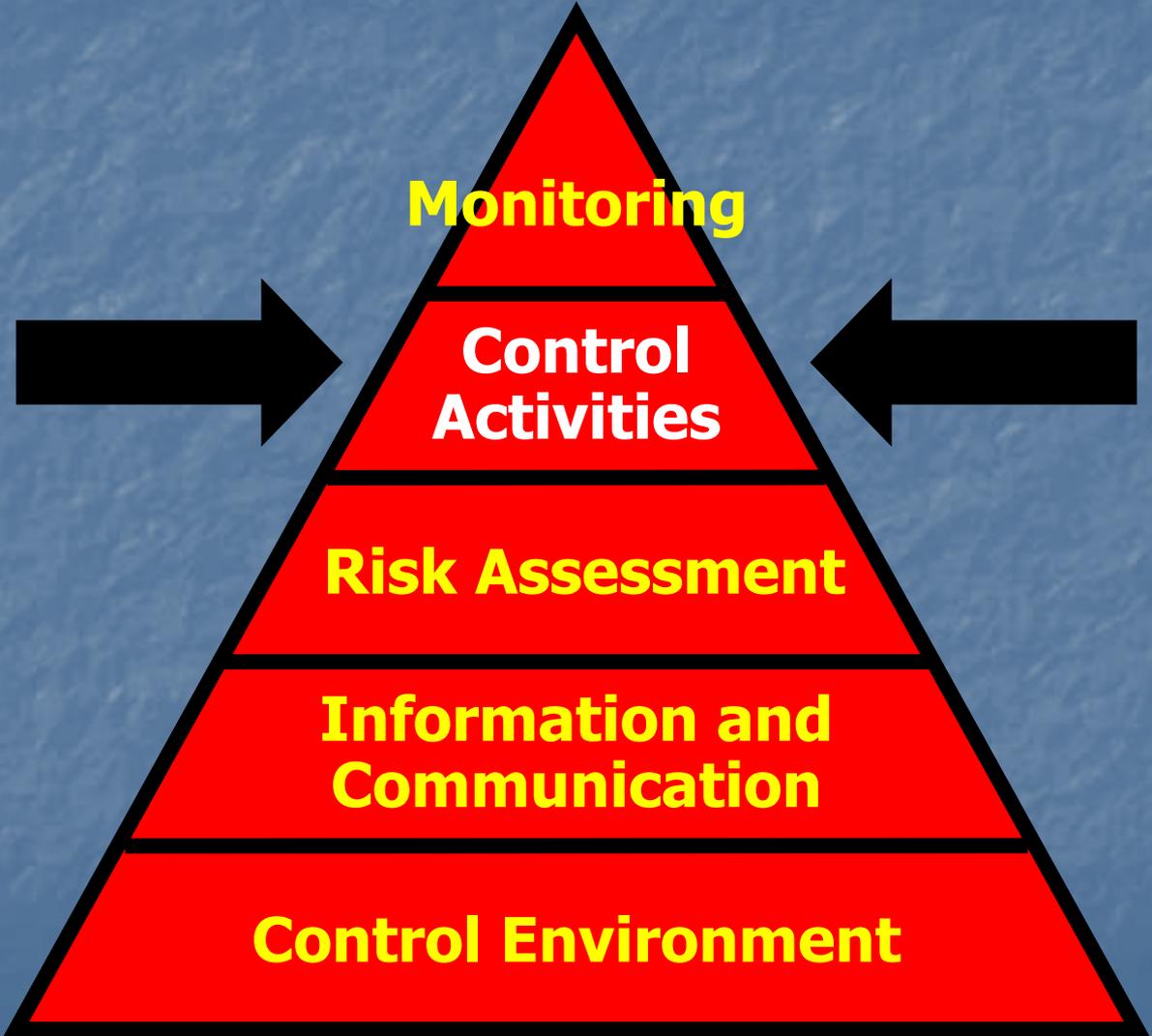
Function: IT Help Desk Telephone Support

A survey asks employees to quantify the impact and likelihood of each event. Events and average scores appear below – events are identified by letter on the risk map.

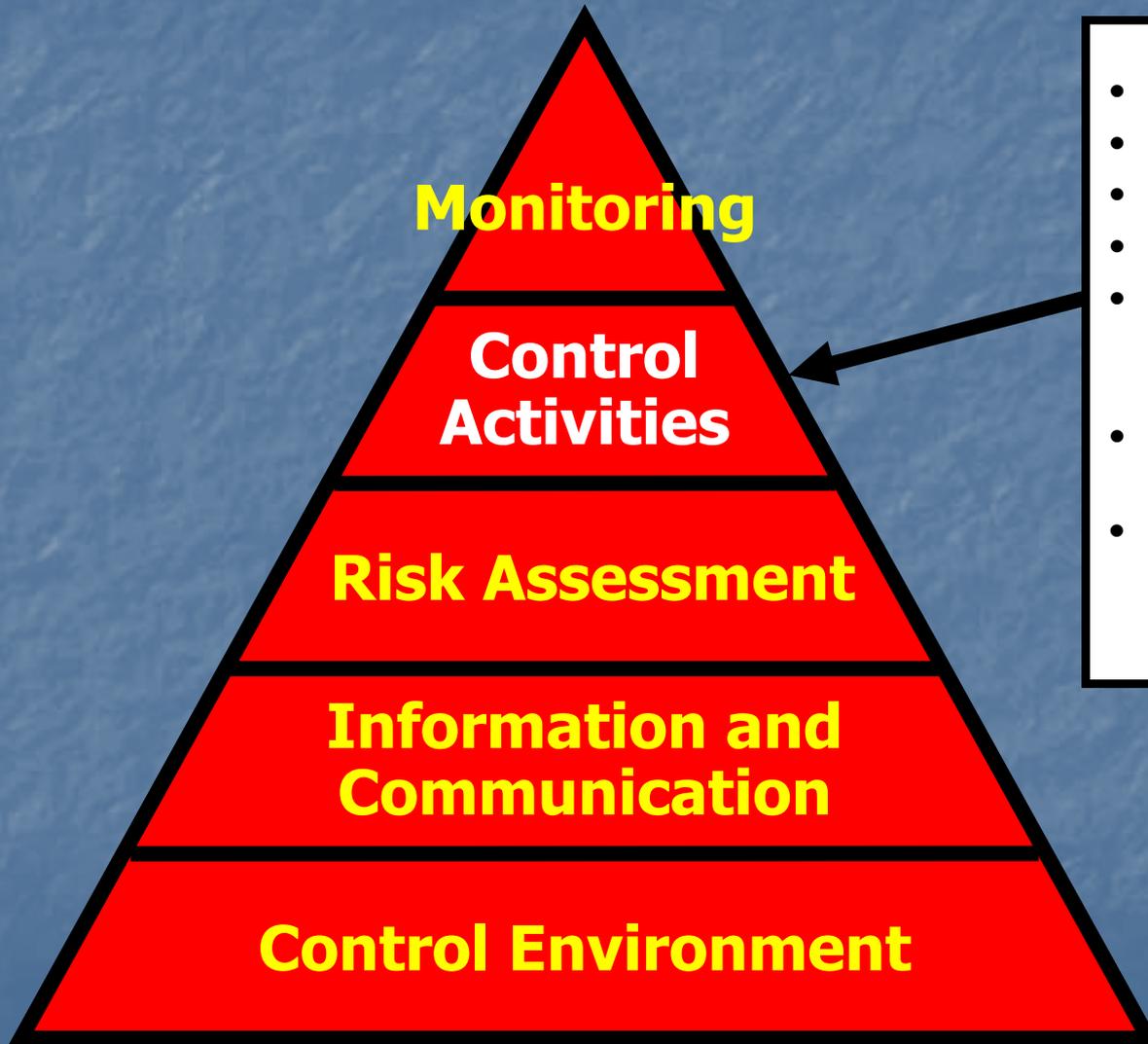
Event	Significance	Likelihood
A. Callers having long waits	7	9
B. Information capture errors	8	2
C. Insufficient staff to handle calls	9	6
D. Loss of telephone services	8	4
E. Loss or corruption of database	9	4
F. Lost record of calls received	3	3
G. Low employee morale.	4	2
H. Malicious or fraudulent calls	3	1.5
I. Repeat calls for the same problem	3	9



First COSO Internal Control Model



Internal Control vs Internal Controls

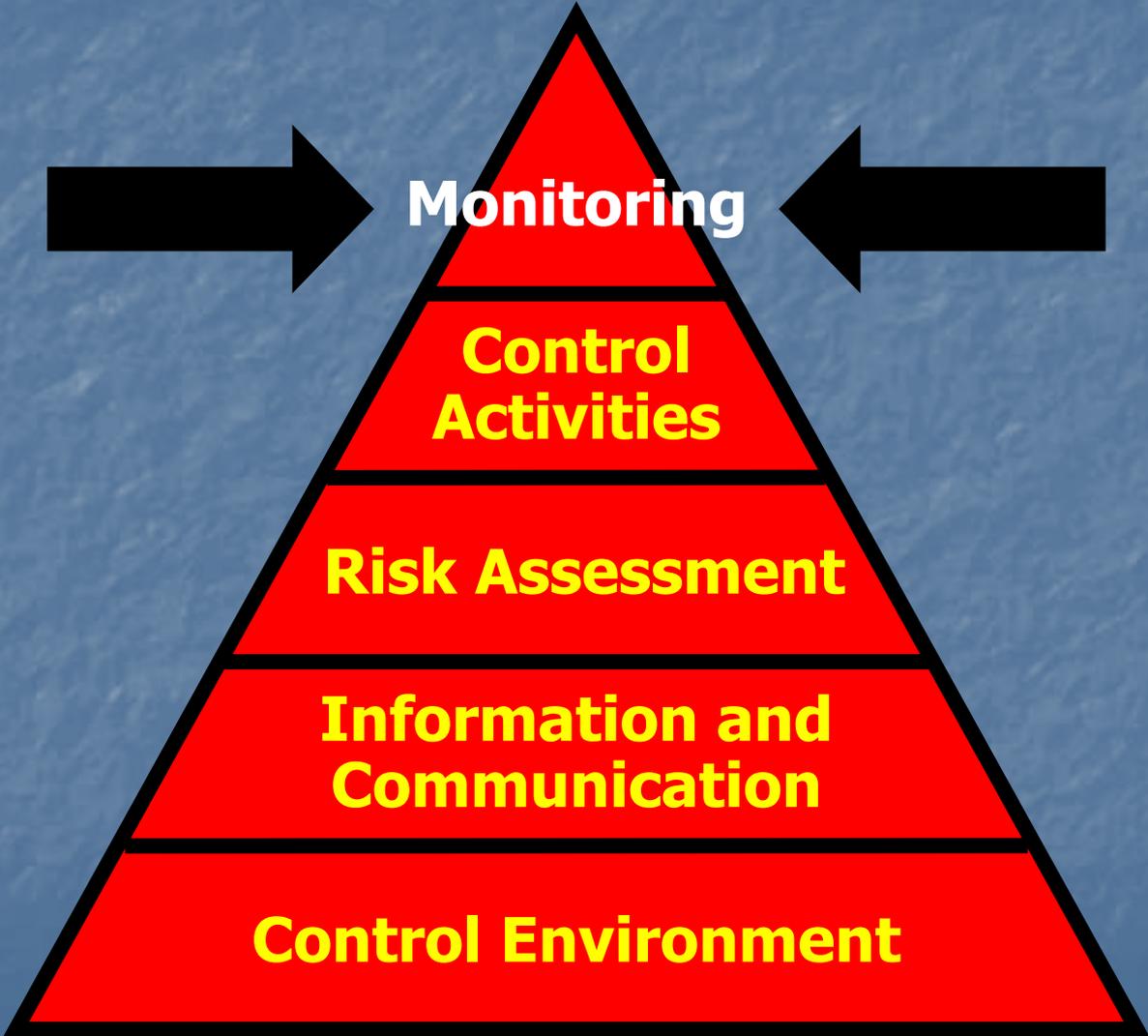


- **Separation of duties**
- **Training and supervision**
- **Authorization and approval**
- **Review and reconciliation**
- **Physical security over facilities, assets, personnel, paper documents, and electronic data**
- **Security over confidential records**
- **Documentation of policies, procedures,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

First COSO Internal Control Model



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.



COSO's Enterprise Risk Management Integrated Framework

Definition of ERM

ERM is a process, effected by an entity's board, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. Components of ERM include the internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring.

Key points appear on the next slide.

Definition of ERM – A Process:

- Regarding achievement of objectives
- By board, management and other personnel
- Applied in strategy setting
- Applied across the whole organization
- Identifies risk “events”
- Manages risk
- Provides reasonable assurance

ERM vs. Internal Control

8 components in new COSO ERM framework:

1. Internal Environment
2. Objective Setting
3. Event Identification
4. Risk Assessment
5. Risk Response
6. Control Activities
7. Information and Communication
8. Monitoring

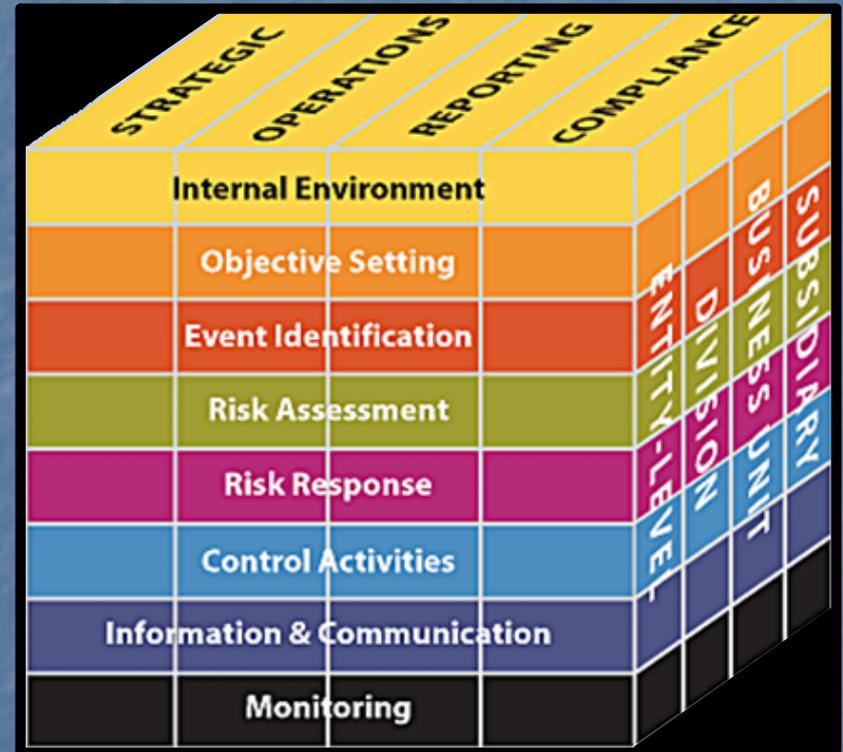
ERM vs. Internal Control

8 components in new COSO ERM framework:

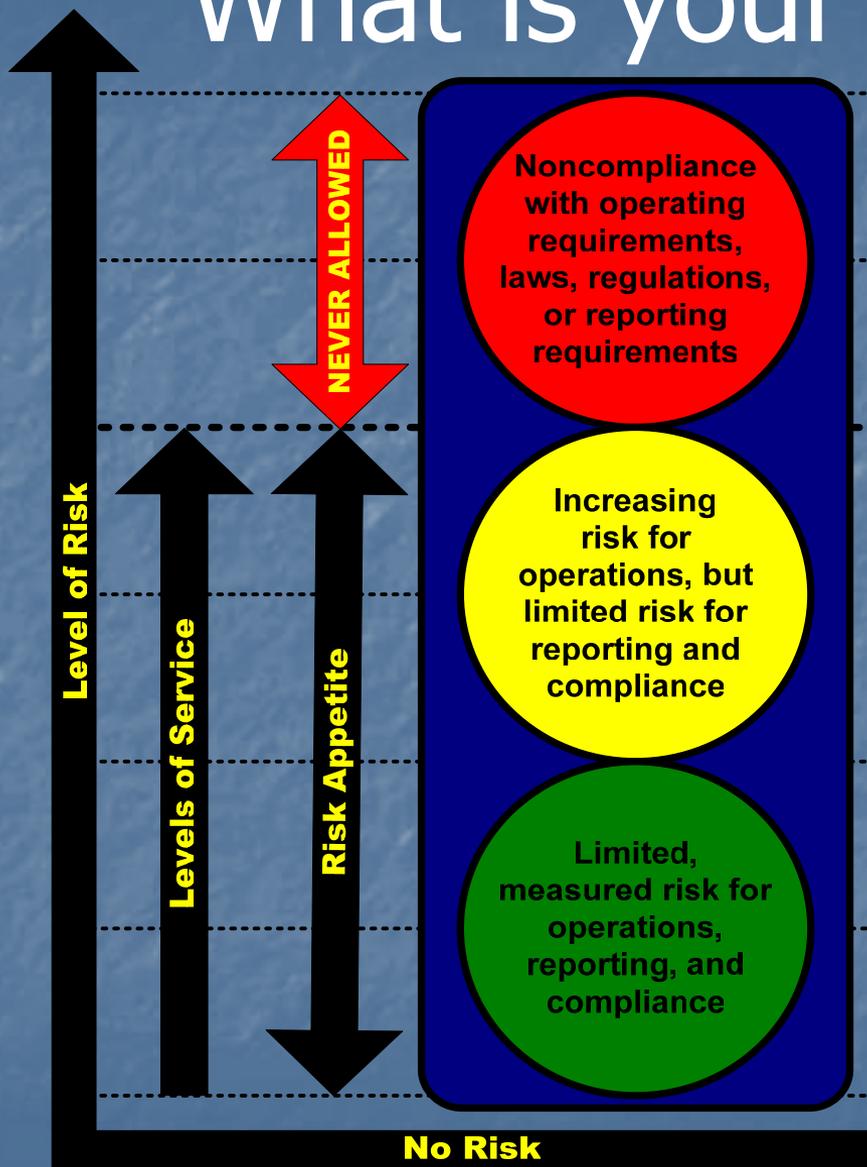
1. **Internal Environment**
2. Objective Setting
3. Event Identification
4. **Risk Assessment**
5. Risk Response
6. **Control Activities**
7. **Information and Communication**
8. **Monitoring**



Old Model vs. New Model



What is your risk appetite?



- COSO models portray private enterprise, where risk-taking is more discretionary than in government.
- Government must not risk either reporting or compliance objectives.



Risk Management Approach and Tools

Evaluating Internal Controls

- Meaningful evaluation of internal controls is the key to prevention of fraud, waste, and abuse.
- Must use due diligence.
- Must document control activities.

Evaluating Internal Controls

- The agency head leads a meaningful management evaluation of internal controls as a key activity to prevent fraud, waste, and abuse.
- Management must use due diligence.
- Management must document its evaluation.

“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

Hard Control vs. Soft Control

	<u>Hard Control</u>	<u>Soft Control</u>
Control Environment	A code of ethics exists	Management acts ethically
Risk Assessment	A strategic plan is prepared	Employees are familiar w/plan
Control Activities	A signatories list exists	Employees know signatory limits

Hard Control vs. Soft Control

Hard Control

Soft Control

Information &
Communication

Exception reports
are run and sent
to management

Exception reports
are reviewed,
understood, and
investigated

Monitoring

Subsidiary
records are
reconciled to
general ledger

Employees make
suggestions on
better ways to do
things

Risk Management Tools

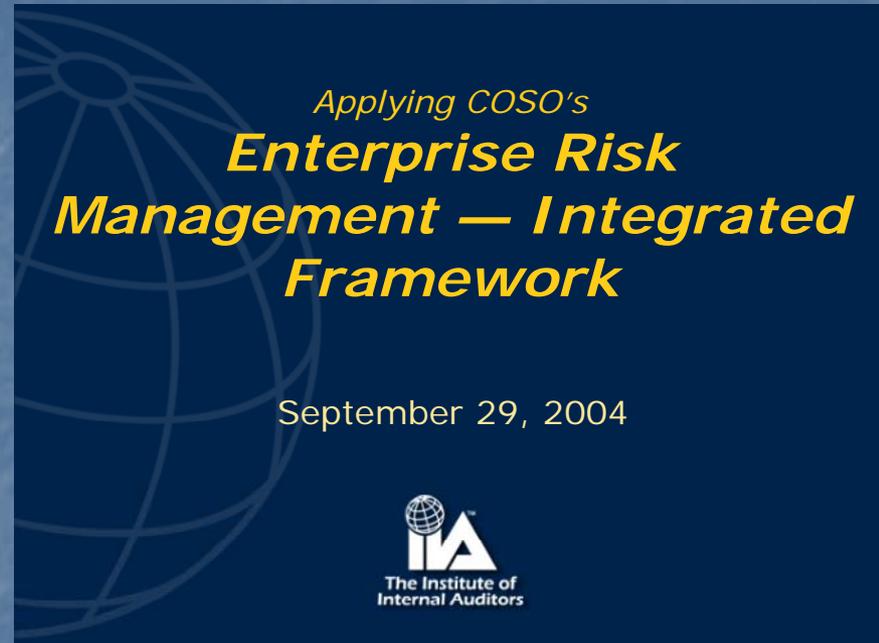
- Control Self-Assessments
- Checklists
- Questionnaires
- Custom tools (e.g., ARMICS appendices adapted from COSO for fiscal programs)

COSO ERM Tools

- Download a free IIA slideshow - “Applying COSO's ERM – Integrated Framework” from

www.coso.org/publications/erm/coso_erm.ppt.

- Review COSO's web site for other reference materials and tools.



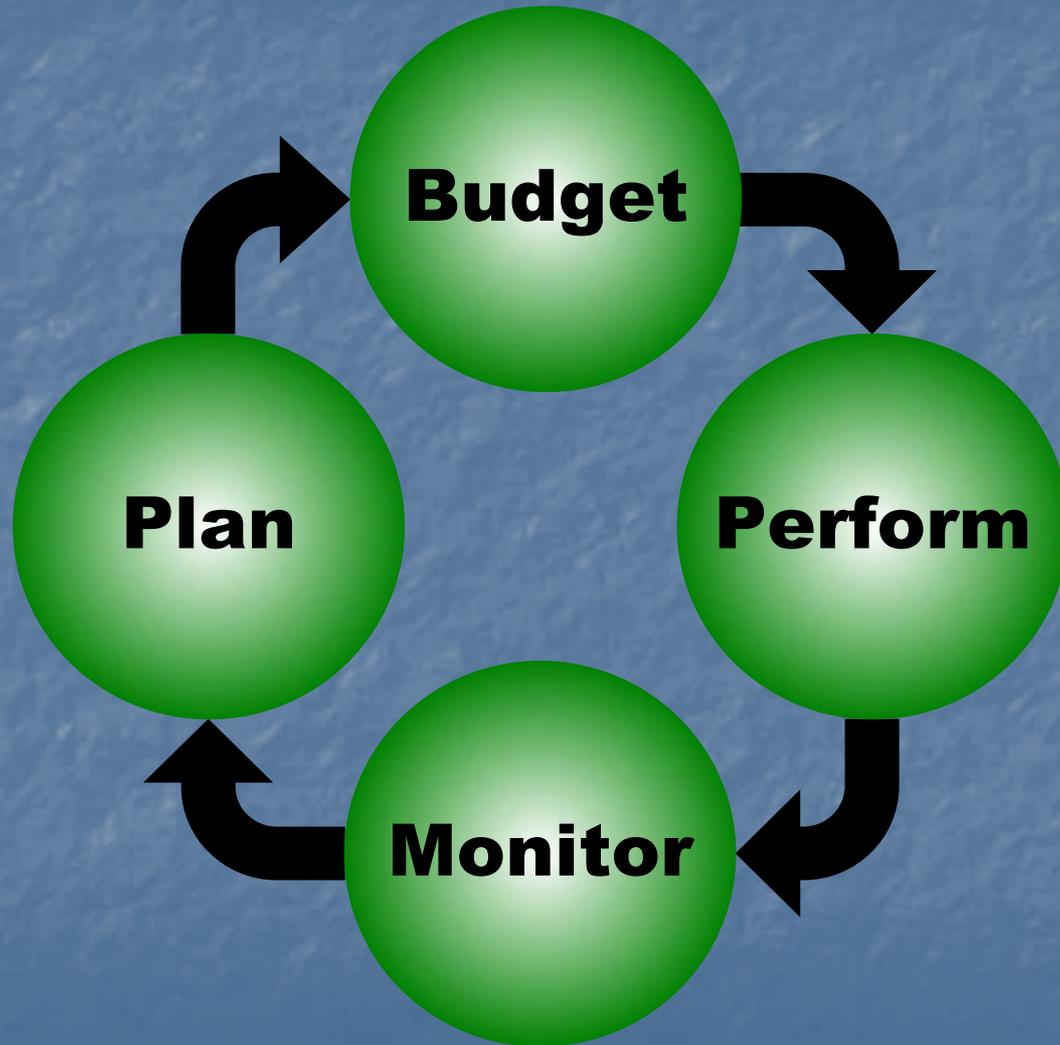
Some ERM tools at www.theiia.org

- 2 free position papers
- 9 seminars
- 10 books
- 5 free reference downloads
- Links to many other resources



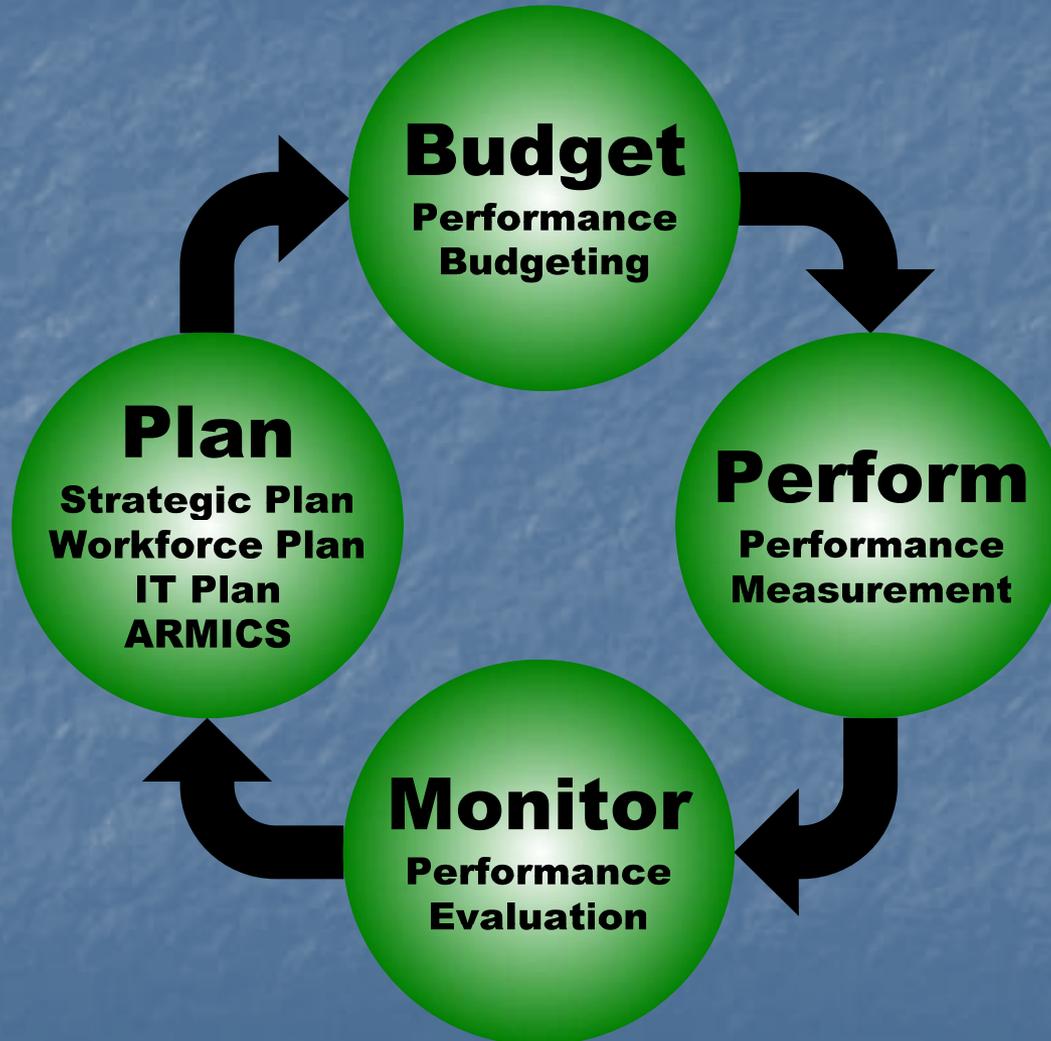
ARMICS and Strategic Planning

The Management Cycle



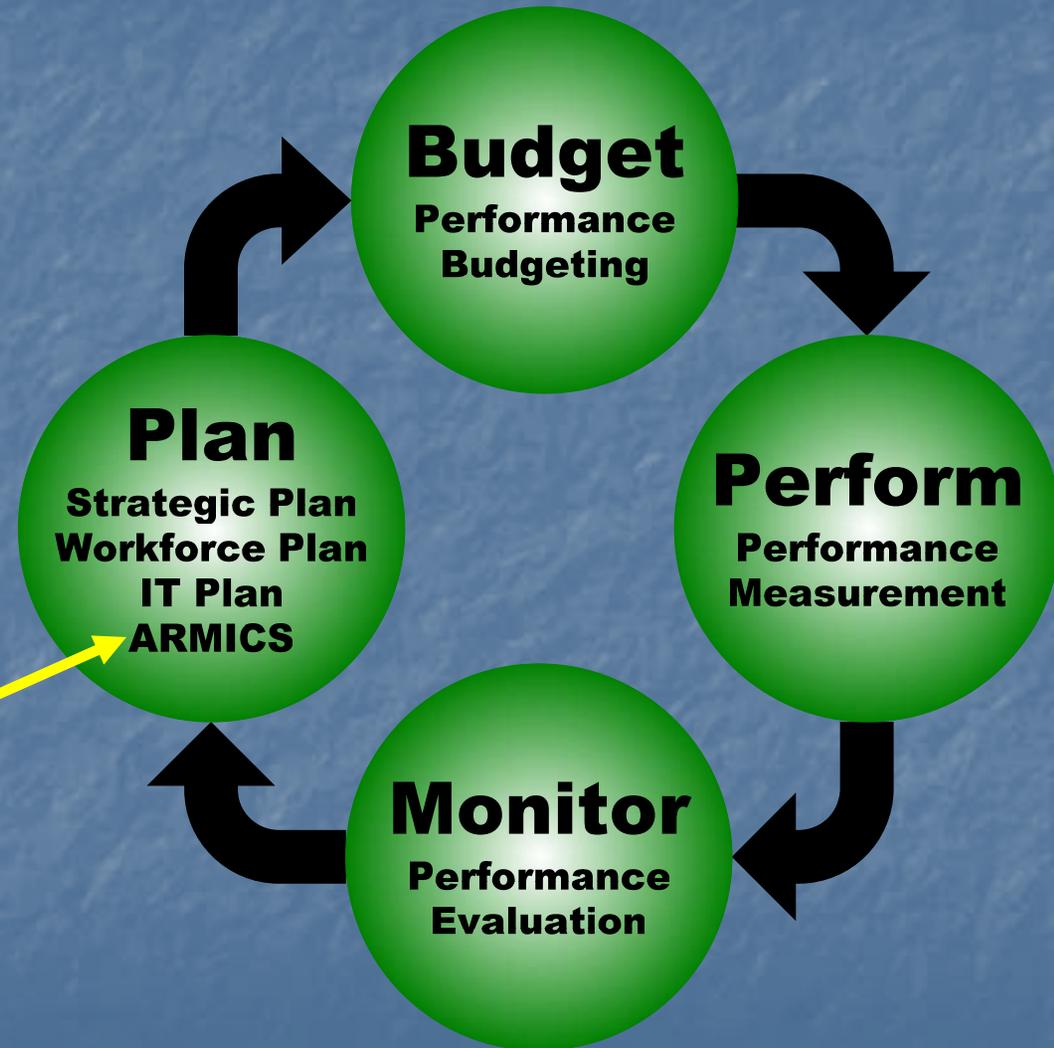
The Management Cycle

Reflecting Strategic Planning, Performance Management, ARMICS, and other COV processes



The Management Cycle

Risk management is “the next logical step” in strategic planning and performance-based management. Strategic plans contain objectives – risk management determines “what could go wrong” in pursuit of those objectives and anticipates those possibilities. As the plan is implemented, the risk assessment directs action if a threat arises to the achievement of any objective.



References

The draft Comptroller's Directive and Agency Risk Management & Internal Control Standards are available from <http://www.doa.virginia.gov>

Contacts

armics@doa.virginia.gov

804-225-4366 – voice

804-225-4250 – facsimile

U. S. Mail:

General Accounting / ARMICS
Virginia Department of Accounts
P. O. Box 1971
Richmond, VA 23218-1971