Risk Management Workshop

Office of the Comptroller

Objective

To:

- Identify your chief goals and objectives
- Identify risks
- Prioritize the risks to achieving objectives
- Determine which controls/processes to review

In order to:

Develop an effective Internal Control Plan by application of the Enterprise Risk Management (ERM) process

Agenda

What is (Enterprise Risk Management) ERM?

The ERM Framework

Objective Setting

Navigating Risk

Identifying Controls to Mitigate Risk

Information & Communication

Monitoring

The Internal Control Plan

Summary

ERM

What is ERM?

Enterprise Risk Management (ERM) coordinates controls to mitigate risks that could keep you from achieving your objectives.

The ERM Framework

The ERM Framework

We recommend the COSO* Integrated ERM Framework.

COSO's Enterprise Risk Management (ERM) is a model structured to integrate risk management throughout an organization.

This ERM structure can help you align your mission and organizational roles within your department's Internal Control Plan.

Employment of the ERM process, improves your ability to meet objectives by strategically addressing opportunities and vulnerabilities.

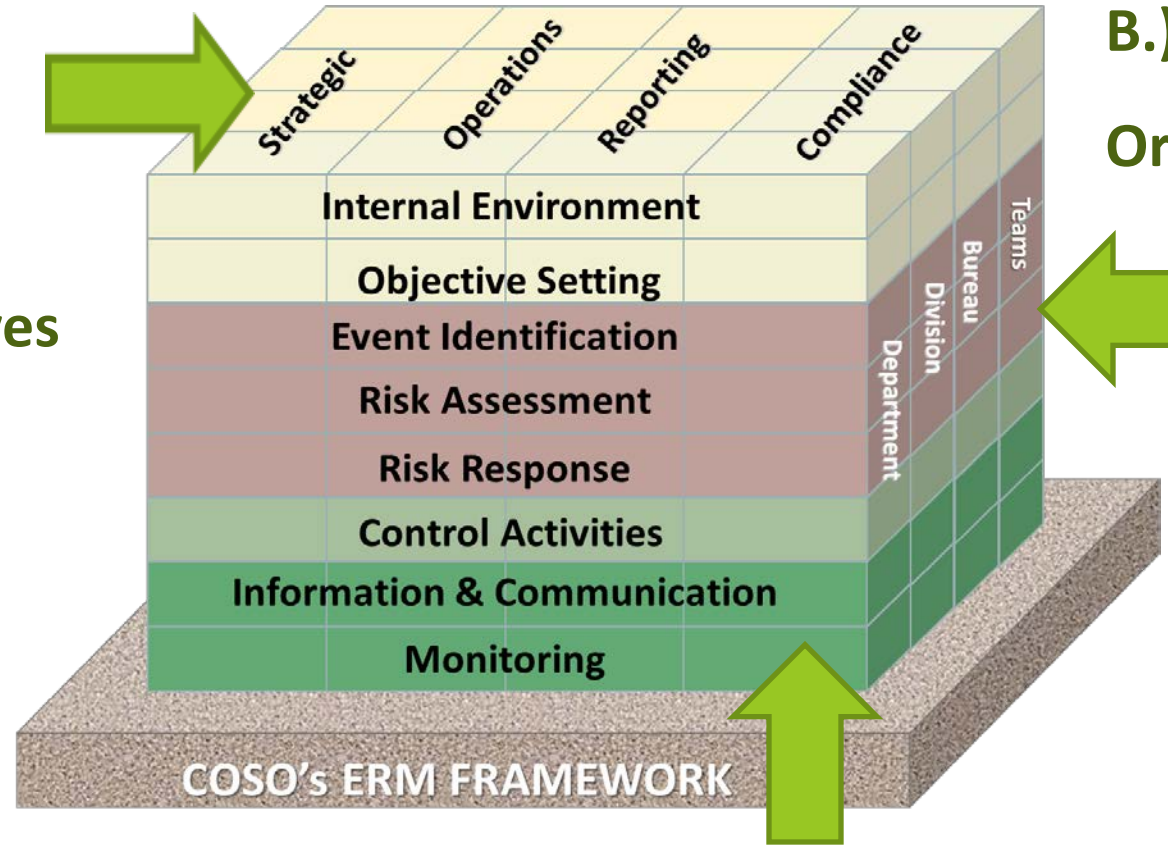
*Committee of Sponsoring Organizations (COSO)

COSO's ERM Integrated Framework

Three levels:

A.)

Mission
Goals
Objectives



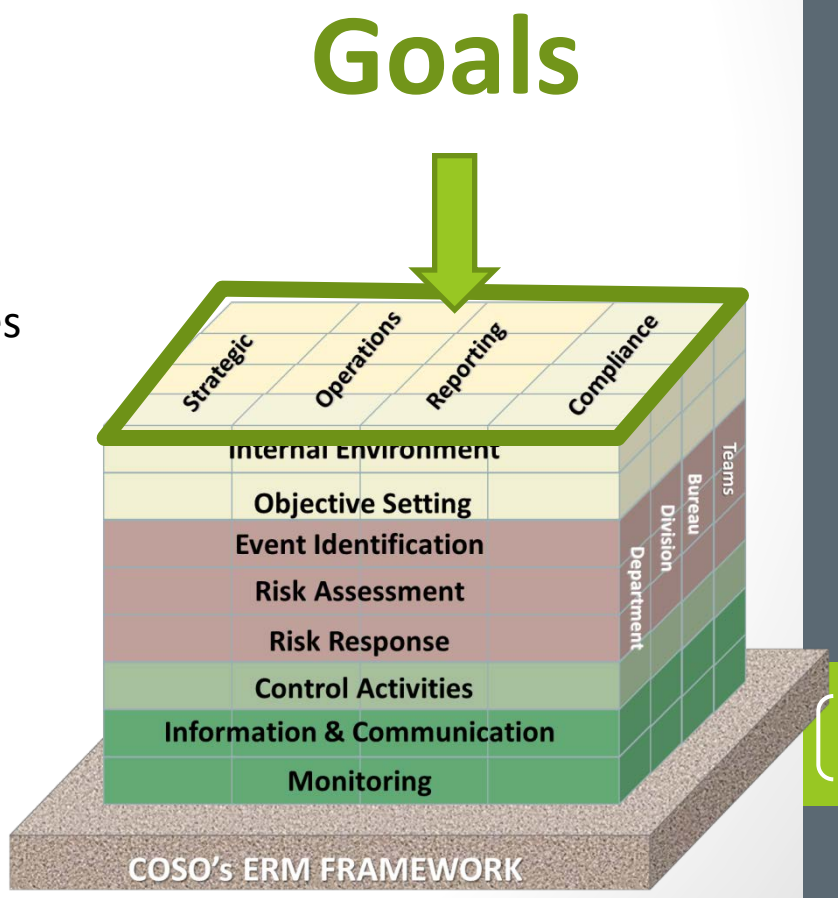
B.)

Organizational Roles

C.) Risk Management / Internal Controls

The ERM Framework
Achievement of Goals/Objectives

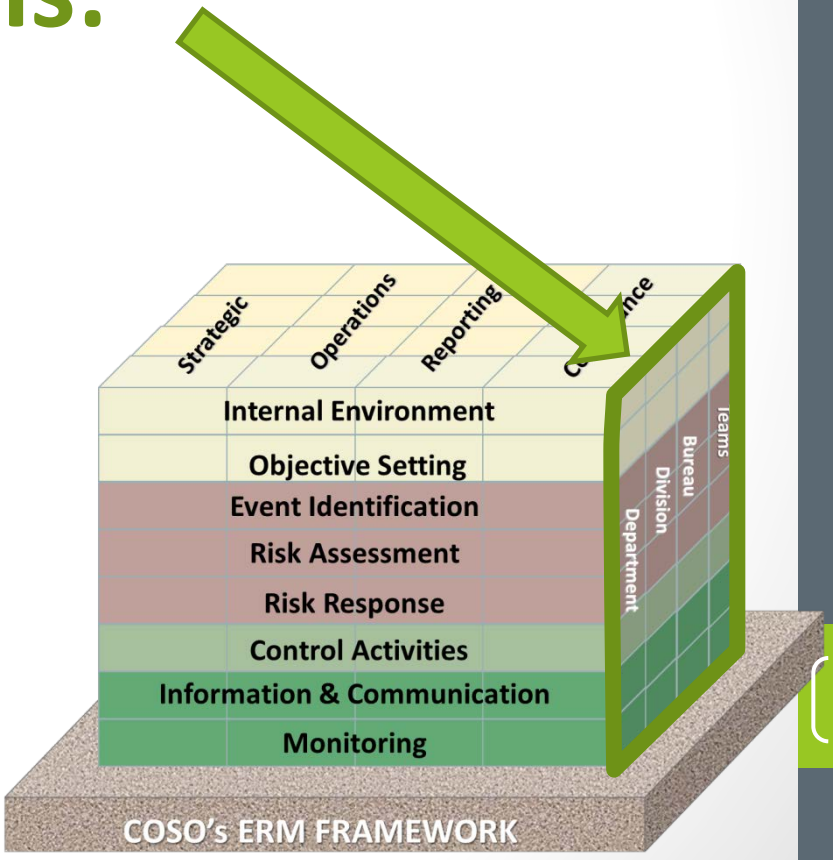
- **Strategy**
  High-level goals, aligned with and supporting its mission
- **Operations**
  Effective and efficient use of its resources
- **Reporting**
  Reliability of reporting
- **Compliance**
  Conformity with applicable laws and regulations



The ERM Framework

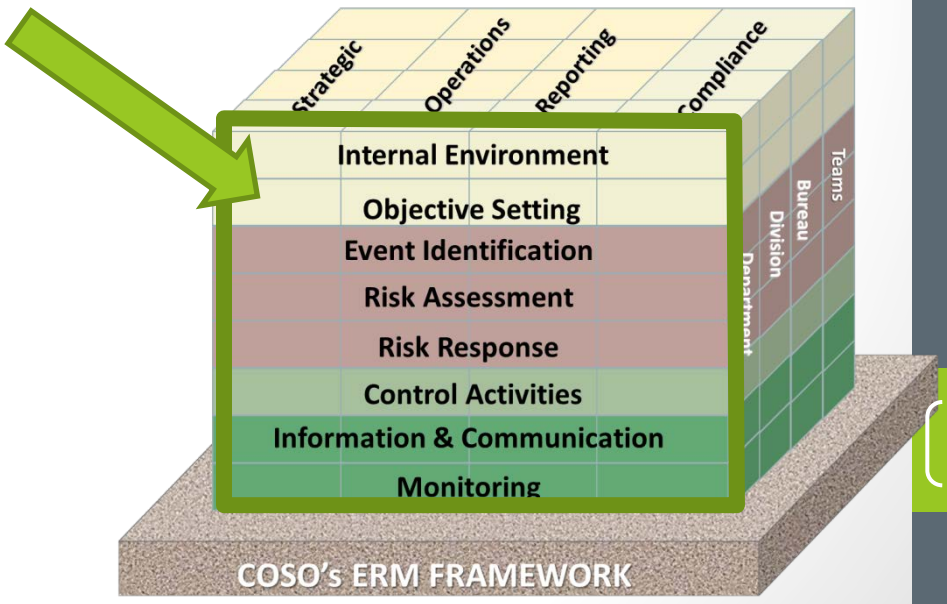
ERM coordinates organizational activity at all levels:

- Department
- Division
- Bureau
- Team



The ERM Framework

Risks are considered through eight interrelated components of the framework.



Internal Environment

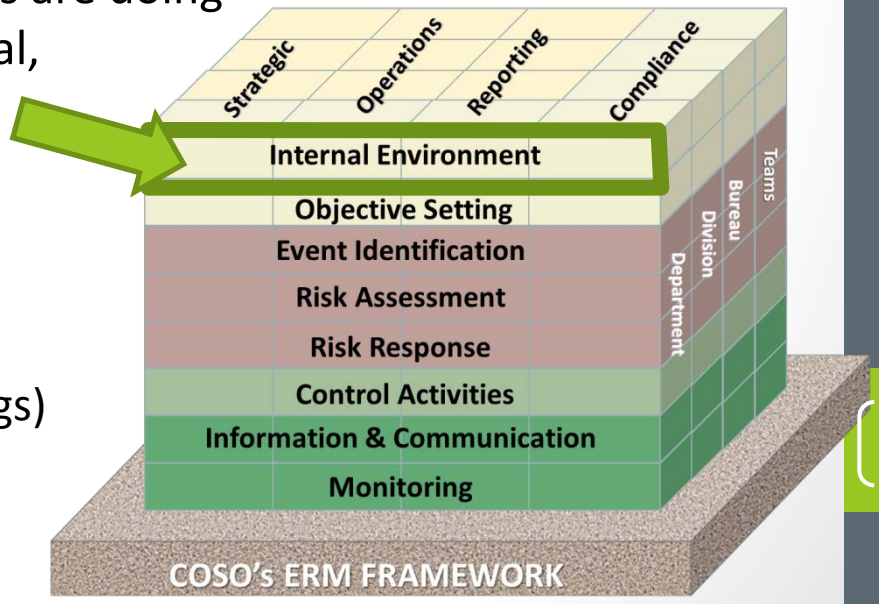
The ERM Framework
Internal Environment

Management Responsibilities:

- Communicates the **mission and goals**
- Conveys the importance of integrity, competence and internal controls
- Provides structure
- Train workforce

Tone at the Top

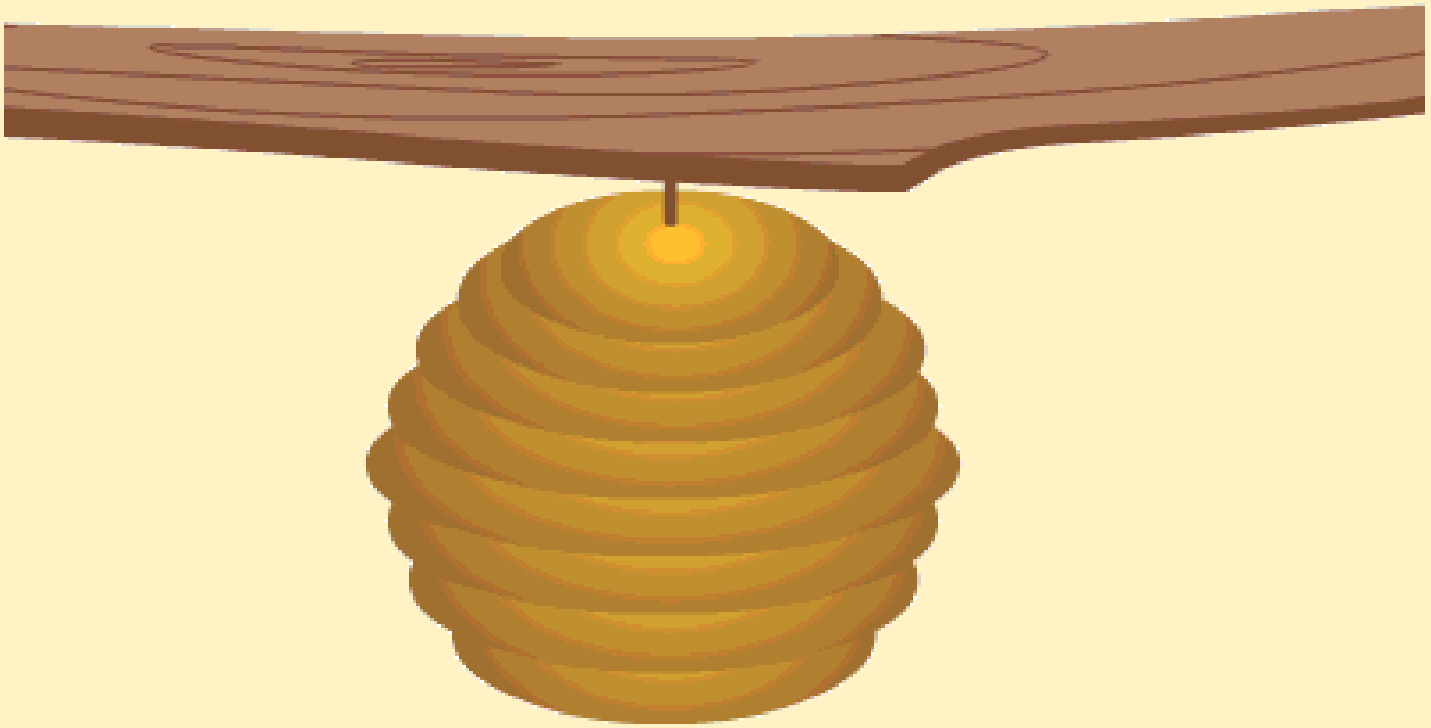
- Employees witness what their bosses are doing
- Zero tolerance for unlawful, unethical, or questionable behavior
- Reward employees for integrating personal and organizational loyalty
  - ✓ Document It (Policies and Procedures, Memos)
  - ✓ Communicate It (Meetings, Trainings)
  - ✓ Demonstrate It (Lead by Example)



What's your Mission?

- **Tells the fundamental purpose of an organization**
- **Specific to the principal reason an organization exists**
- **Creates value**

Where do you see yourselves, as part of the mission?

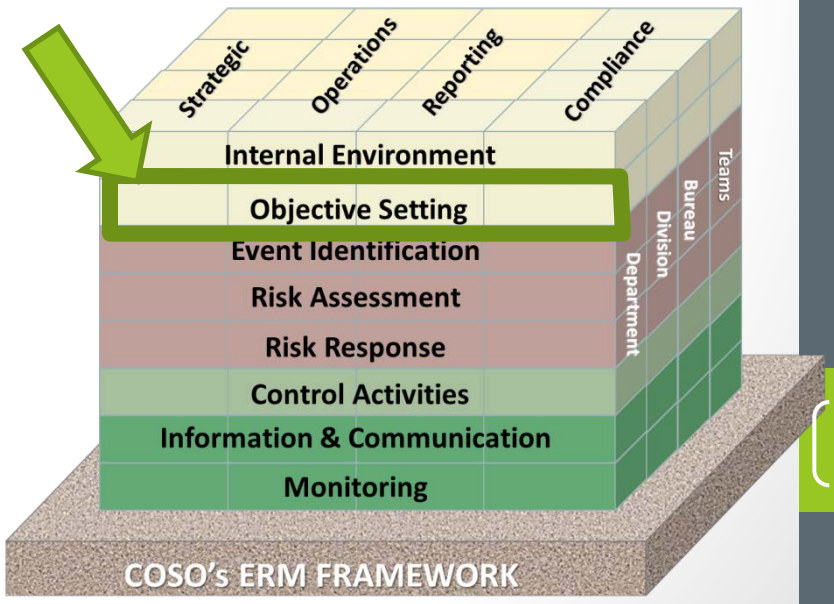


Objective Setting

The ERM Framework
Objective Setting

- Objectives must exist before management can identify potential events affecting their achievement.

- Have a process in place to set objectives that support the entity's mission and are consistent with its risk appetite.

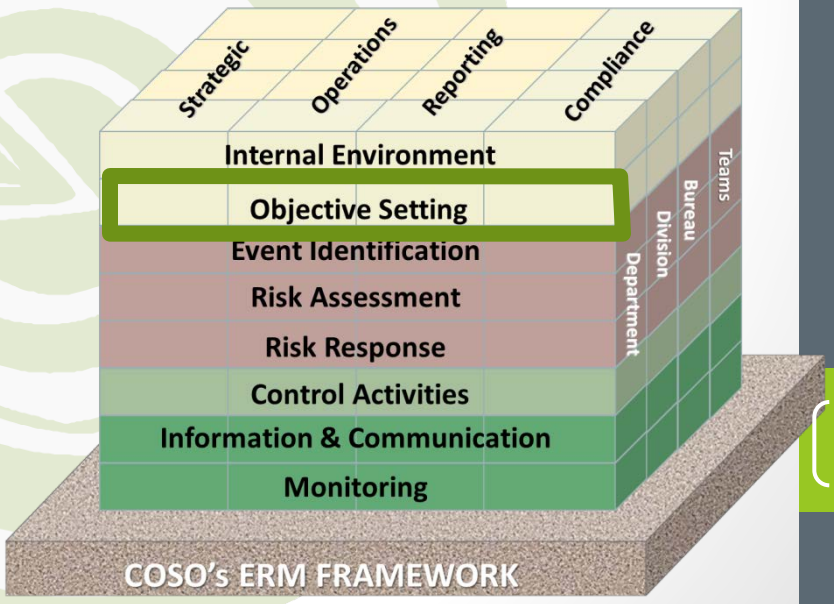


Objectives are based on goals

Goals are high level

Objectives are **SMART**:

- **S**pecific
- **M**easurable
- **A**ttainable
- **R**esults focused
- **T**imely



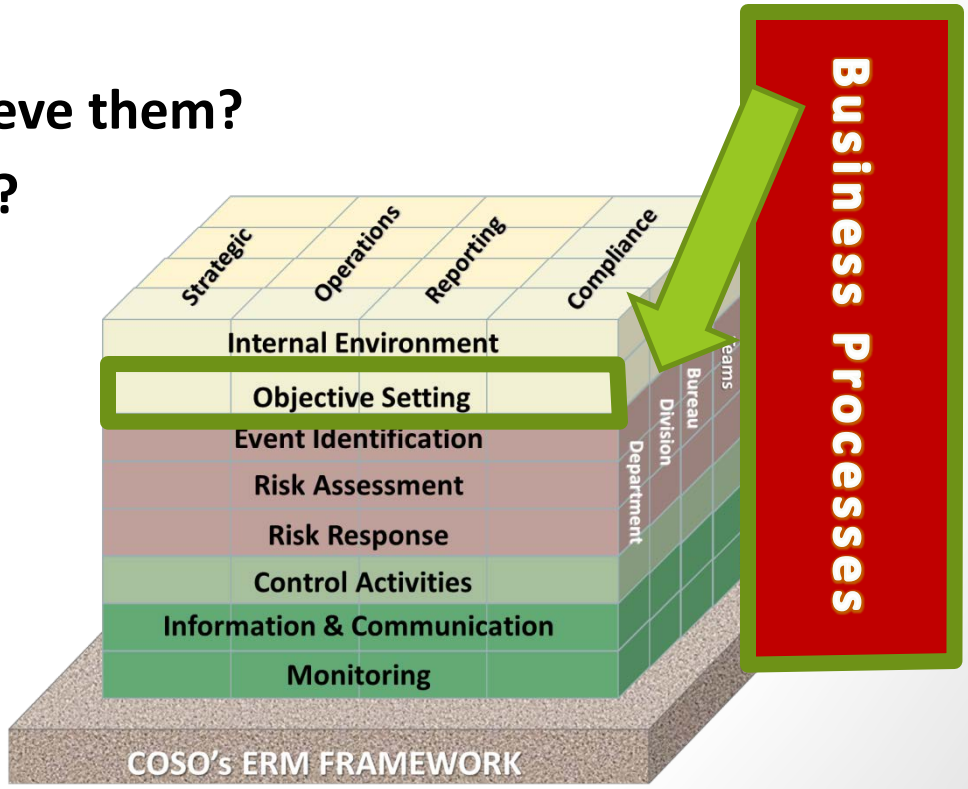
Prioritizing what you do

Finance and Administration determines and prioritizes goals for its business processes:

What are the goals?

What are the steps to achieve them?

Which are most important?



Activity

Handout

- Mission Statement:
- My Business Area:
- What I do:
- Goal:
  - Objectives (step toward the goal)
  - Objectives (step toward the goal)
  - Objectives (step toward the goal)


Navigating
Risk

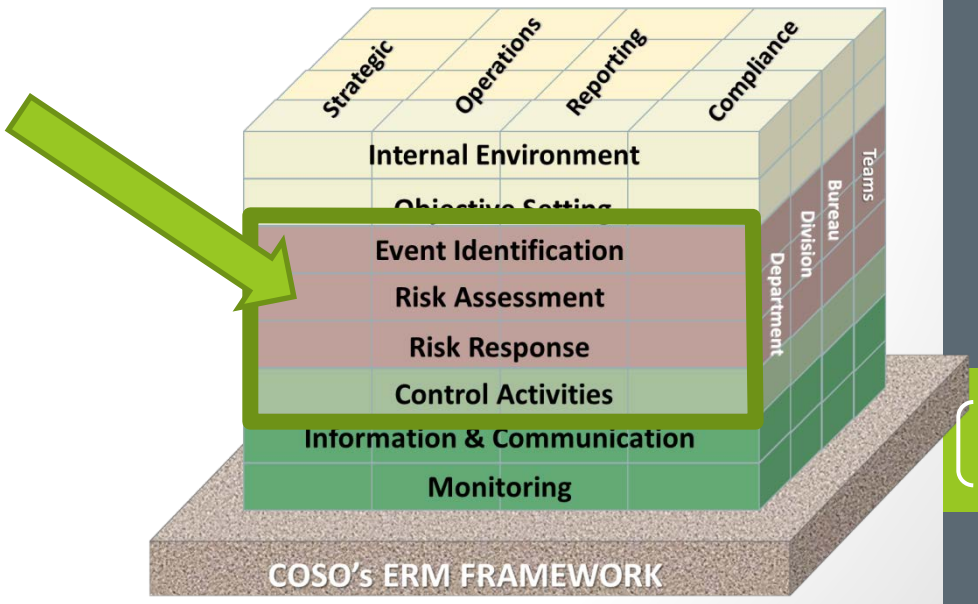
Risk Never Sleeps

- Risk is a fact of life; life constantly changes and is uncertain
- All management is essentially risk management

- Many risk management activities are well defined and accountability has been assigned
- Risks that have not been defined/assigned, may “slip between the cracks” and/or be managed inconsistently due to individual perceptions of the significance of the risk.

Back to the Framework

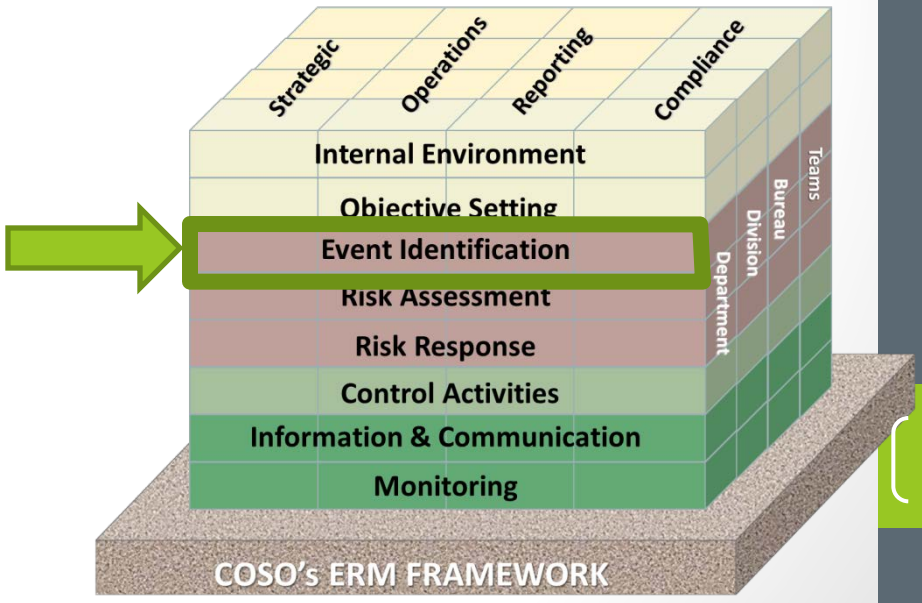
Risk Management / Internal Controls



Risk Identification

The ERM Framework
Event Identification

- Internal and external events that impact achievement of objectives must be identified, distinguishing between risks and opportunities.
- New opportunities are channeled back to management's strategy or objective-setting processes



Red Flags

- Two Parts:
- Risk Identification – Identify Risk
- Identify the Red Flags
- Red flags are indicators are activities that may indicate trouble in any process.
- These are best described as clues or hints that something outside the norm is occurring or has occurred and that a closer look at an area or activity is required
- They are trigger points that something needs to be done

Types of Risk

Internal Hazards

Cyber Threats

Natural Hazards

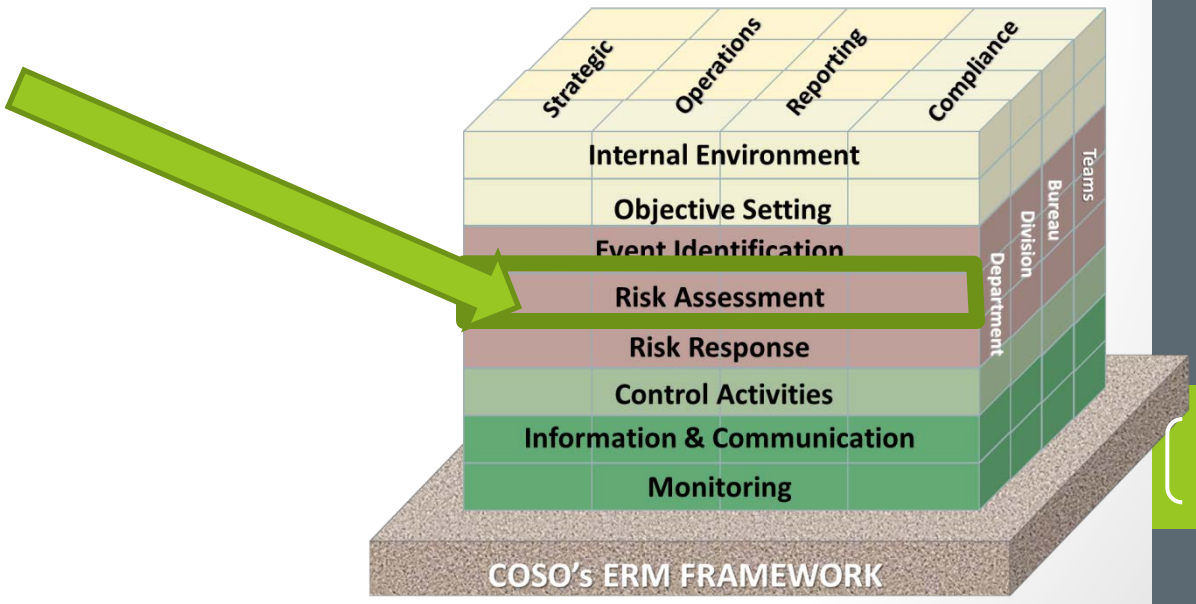
Fraud

Harmon Tower, Las Vegas

Risk Assessment

The ERM Framework
Risk Assessment

- Risks are analyzed, considering likelihood/frequency and impact as a basis for determining how they should be managed.
- Risks are assessed on an inherent and a residual basis.



Risk Assessment: Likelihood/Frequency

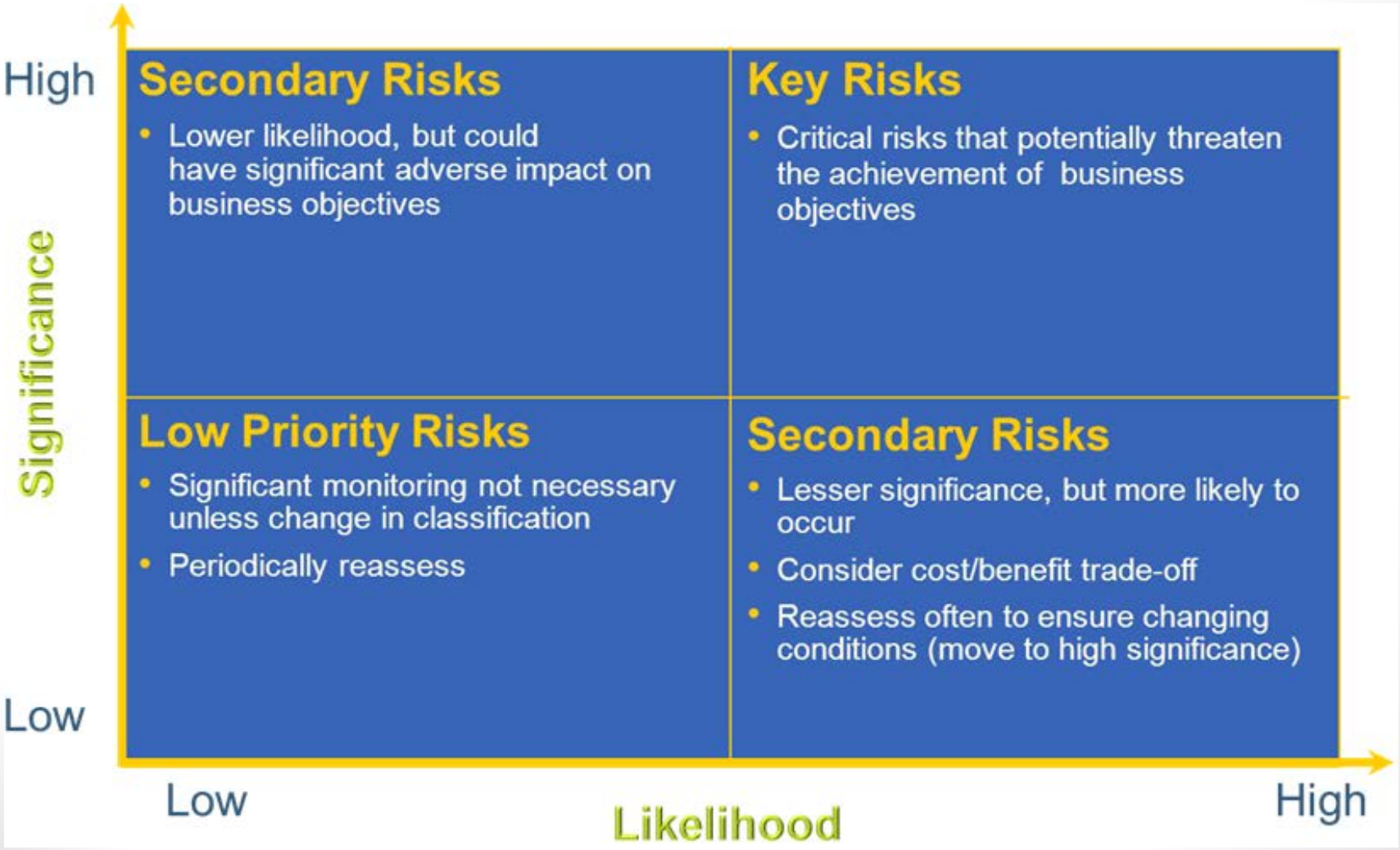
Can it happen? How often?

Likelihood	Comment
Probable	**The event is expected to occur in most circumstances.**
Possible	**The event is more than remote but less than probable.**
Remote	**The event may occur only in exceptional circumstances.**

Risk Assessment: Significance of Impact

Significance	Comment
Major	**Very significant impact that jeopardizes the ability to achieve objective.**
Moderate	**Management gets involved with issue and focuses on completing it within a timely manner.**
Low	**May not require attention of management. Process changes likely not required in response to risk occurrence.**

Risk Rating Interpretation



GOAL:

To treat a risk, you can:

- Avoid
- Accept and Monitor
- Reduce the Likelihood/Impact
- Transfer the risk

Treatment must reflect the:

- Risk appetite of your group
- Amount of control you have
- Values of the group, and
- Be measurable, and time-limited

HEAT MAP	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

Risks:

	LIKELI-HOOD	IMPACT	YOUR SCORE	GROUP SCORE (AVE)	COLOR
Risk 1					
Risk 2					
Risk 3					
Risk 4					
Risk 5					

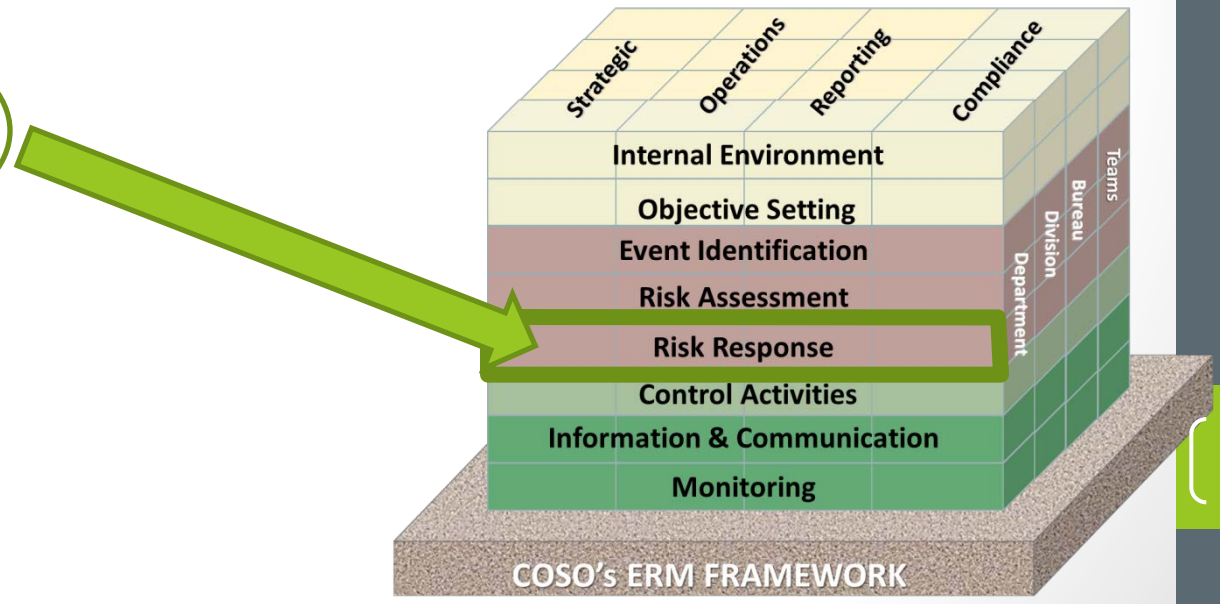
Risk Response

The ERM Framework
Risk Response

Management decides per risk:

Four responses

- ✓ avoid the risk
- ✓ accept the risk
- ✓ share the risk
- ✓ reduce the risk



Control Activities

The ERM Framework
Control Activities

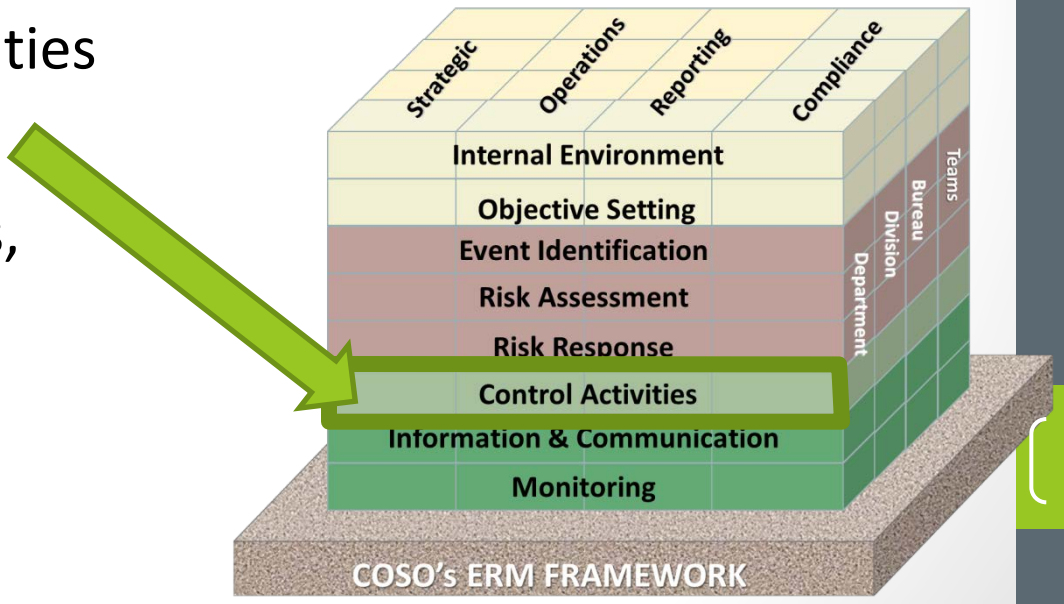
Control activities help assure that risk responses are effectively carried out. These can be federal/state laws or your own policies and procedures.

A. Preventive controls

Segregation of duties

B. Detective controls

Exception reports, reconciliation



Control based approach

Premise: Fires are unavoidable and unpredictable but can be extinguished.

- Install fire extinguishers
  - Install alarms
  - Inspect them regularly
  - Add more as required
  - Report and remedy deficiencies

Root Cause approach

Premise: Fires are predictable and avoidable. Fires are caused when combustible material is exposed to a source of ignition…

- Track all instances of fires and analyze root cause
- Eliminate sources of ignition
- Eliminate combustible material
- Ongoing risk assessments to identify and eliminate the root cause

Control Activity Examples

Risk	Activity
Late payments	Let system schedule the payment date Use correct date stamp
Discounts missed	Check Comptroller reports
Not built to spec	Vetting of vendors Project management Site inspections

Sample Risk Management Chart for Objective: Safe Buildings

Item	Risk Event	Occurrence	Impact	Control	Control Type	Reference
		V=Very Likely	H=High		P=Preventative	
		S=Somewhat Likely	M=Moderate		D=Detective	
		U=Unlikely	L=Low			
Bldg -100	Unauthorized site access	S	H	Photo ID Required	P	Property Management
	Six sites			all sites		Procedures Manual

How Controls Mitigate Risks

Controls do not make risks disappear

- Too many, or ineffective controls, are evidence of poor risk management
- Control management – sometimes less is more

When Do Controls Change?

- Changes in federal/state laws and regulations
- Existing procedures prove ineffective
- Changes due to organizational structure
- Changes in agency priorities

Group Activity

Activity: Risk Modeling

Select a goal, then:

Determine measurable objectives
(What are the steps to get there?)

Identify risk
(What can prevent success?)

Assess risk
(How bad is it?)

Control risk
(What can be done about it & who is responsible?)

RISK MODELING:

Goal:	
Objective:	

Risk	Red Flag	Control

Control Self-Assessments

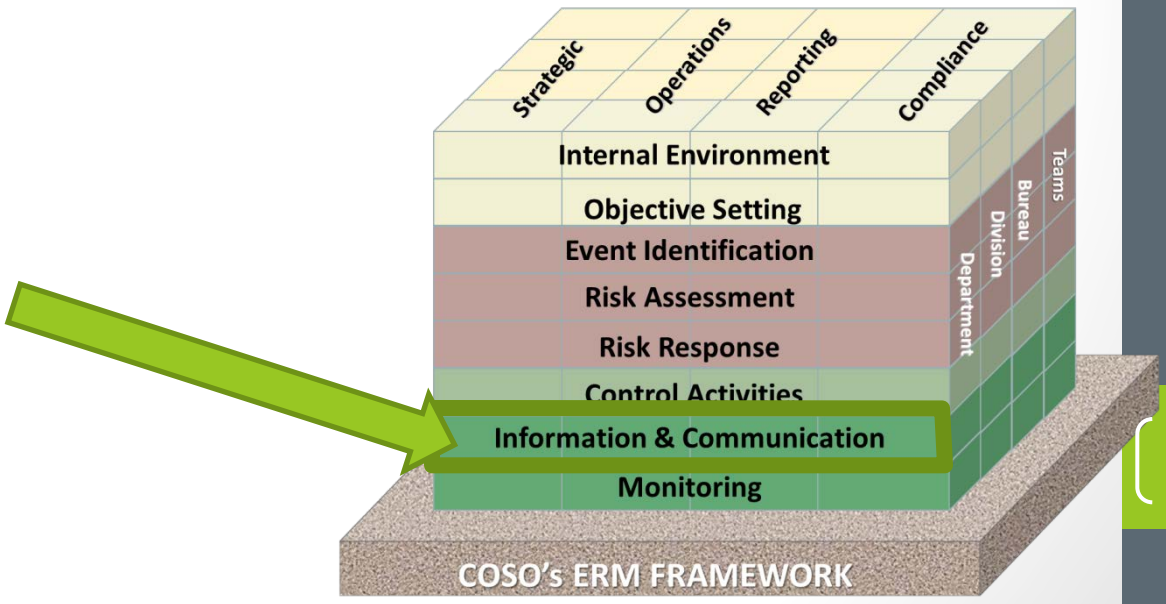
National Association of State Comptrollers (NASC) Multi-State Consortium on Internal Control

- Accounting System Section
- Budgets and Planning Section
- Buy American Act Section
- Capital Assets Control Section
- Cash Section
- Control Environment Section
- Davis-Bacon Act Section
- Information Systems and Technology Section
- Payables Section
- Personnel and Payroll Section
- Receivables Section
- Risk Assessment Section

Information & Communication

The ERM Framework Information & Communication

- Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities.
- Effective communication also occurs in a broader sense, flowing down, across, and up the entity.



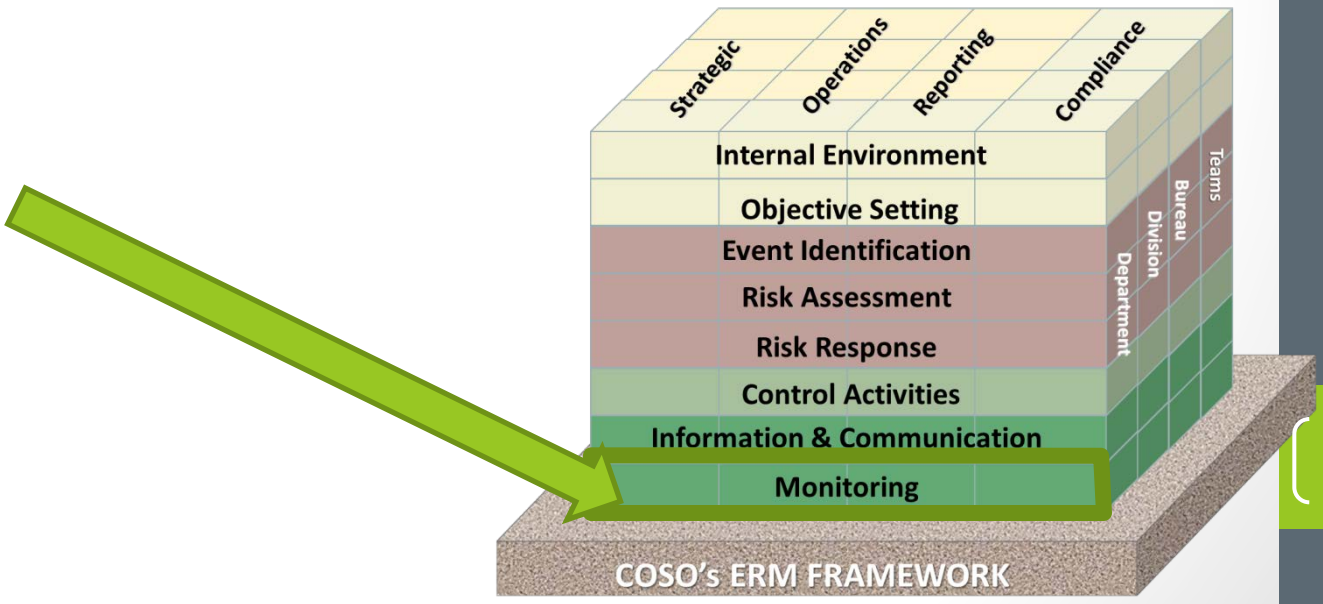
MONITORING

"Even a correct decision is wrong when it was taken too late."

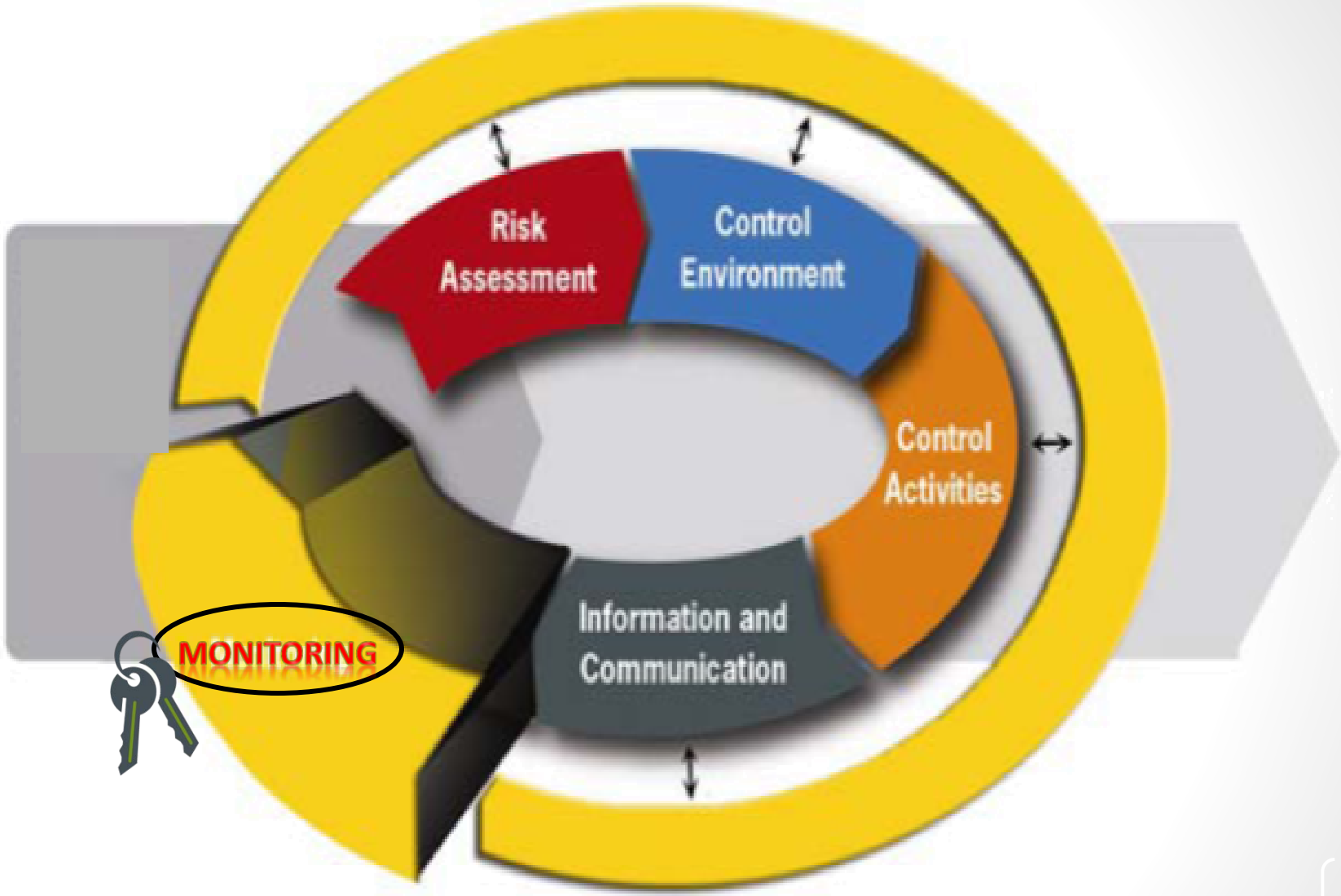
Lee Iacocca, Chrysler

The ERM Framework Monitoring

- The entirety of enterprise risk management is monitored and modifications made as necessary.
- Monitoring is accomplished through ongoing management activities, separate evaluations, or both.



Internal Control Cycle



Monitoring

- Schedule monitoring on a regular basis.
- Test controls at least annually to determine whether they continue to be adequate and are still functioning as intended.
- Use program monitors, auditors and reviewers as a resource in monitoring controls.

Next Steps

The Internal Control Plan

Why Have an Internal Control Plan?

- It's the law
- Great tool for new employees and auditors
- Tells your unique story
- Puts focus on the "Right Stuff" (day-to-day)
- Promotes effectiveness and efficiency

All in Order To:

Accomplish Your Goals and Objectives

Internal Control Plan

An effective Internal Control Plan is a high level, department-wide summarization of risks and controls for all of its business processes.

It is supported by lower level detail, communicated throughout the department, and continuously monitored and updated.

Each department's internal control plan will be unique; however, it should be based on the same framework – the organization's mission statement, goals and objectives, and components of internal control recommended by COSO.

Internal Control Plan

It is not uncommon for the detailed policies and procedures to be modified due to changes in personnel, audit or quality assurance recommendations, etc.

An organization is a living entity which changes over time. As a result, the organization's mission, goals and objectives must be regularly evaluated and periodically revised. Thus, internal control is an ongoing process known as the Internal Control Cycle.

Why add Anti-Fraud plans to your Internal Controls?

According to the Association of Certified Fraud Examiners, (ACFE),in their *2010 Report to the Nations* demonstrated that organizations that invested in Anti-Fraud Action plans halved their average median losses.

Effective Anti-Fraud Action Plans included:

- Hotlines
- Employee Support Programs
- Enforceable Codes of Conduct
- Adherence to proper "Tone at the Top"
- Fraud Training
- Formal Segregation of Duties
- Job Rotation

What's Not in the Plan … but?

- Detailed daily activities
- Every objective and risk event
- Detailed Risk Assessment – refer to
- Strategic Plan – refer to
- Policies and Procedures – refer to
- Disaster Recovery Plan – refer to

SUMMARY

Summary

- Evaluate mission and goals/objectives
  - Include all programs/activities
- Risk
  - ID events that threaten success
  - Assess
  - Respond
- ID controls to mitigate risk
  - Implement activities to support controls

Always Segregate Duties

Put another way:

- What are you trying to accomplish?
- What could prevent you from doing that?
- What policies & procedures could you put in place to decrease this risk?
- Who else needs this information?
- How can you tell if these policies are working?

Next Steps – the Nitty Gritty

- Establish and continuously update your internal controls
  - Follow 0guidelines
  - Identify risks and how you mitigate them
- 5 elements must be addressed
  - Control environment – “tone at the top”
  - Risk assessment
  - Control activities
  - Information and communication
  - Monitoring

Next Steps – the Nitty Gritty

- A point person or group needs to be named to manage the internal controls and be responsible for it
  - Update policies and procedures
  - Monitor changes in grant regulations
  - Communicate to program personnel
  - Follow up on all deficiencies

Risk Never Sleeps

Contact us @: