



Contractor Internal Audit Directors (CIAD) Conference  
*"Speak Up In Spokane"*

# Ethics & Compliance/Control Frameworks and Testing

**RICK KOFMEHL**

Washington River Protection Solutions  
Spokane, WA

# CAE, Ethics and Compliance Officer

## Rick Kofmehl

25+ years of professional experience in audit, finance, accounting and operations

Currently Washington River Protection Solutions CAE

10 Years Boeing aircraft, space and defense experience

- Senior Manager Boeing Corporate Audit
- Enterprise Wide **SOX** Financial Controls Assessment/ Testing
- Audit Operations Processes Tools and Training
- Enterprise Wide Compliance and Risk Assessment/Testing- Boeing Commercial, Space and Defense
- Responsible leader for audit advisory processes and execution
- International and domestic assurance for compliance and operational effectiveness



**Jefferson Wells Consulting lead manager**

- Business Combination of McDonnell Douglas Finance Corporation & Boeing Capital Corporation \$9 Billion Portfolio
- Implementation of financial controls and enterprise wide application for control tracking and evaluation



**Various companies**

- Senior Manager/Consultant/Controller/Public Accounting & Advisory projects/Operations



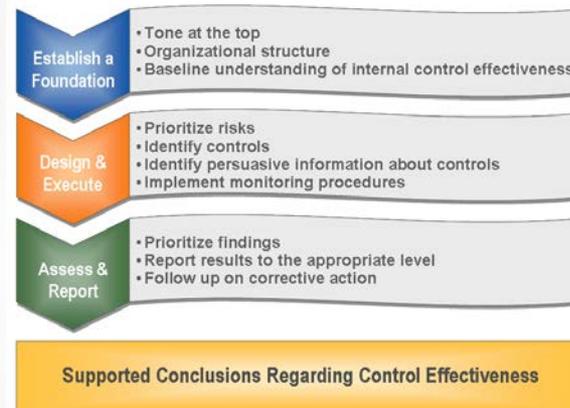
**Education**

- MBA, Business and Technology Management University of Washington
- B.S. Accounting
- Licensed CPA
- Certified Internal Auditor



# Presentation Objectives

- Demonstrate Control requirements for Public Companies vs Government Contractors
- Understanding the benefits of Ethics & Compliance
  - Play offense
  - Protect company and management team
  - Provide a competitive advantage for future contracts
  - Move to a more positive open culture
- The purpose for the adoption of a uniform control framework (COSO)
  - Provides systematic approach and basis for assurance
  - Supports OMB, GAO, IG and DOE recommendations/objectives
- Provide essential element for control execution / risk events



Copyright © 2009, The Committee of Sponsoring Organizations of the Treadway Commission (COSO)

# Ethics and Compliance Considerations

- Securities and Exchange Commission Regulations
- Parallel to Government control requirements
- Competitive Advantage – Boeing Example
- DOJ requirements for reduction in culpability scores
- Ethics and Compliance
- Control Framework
- Evaluation/Testing



COMPLIANCE  
Checkup

# Required of All US Public Companies

## 85 SECURITIES EXCHANGE ACT OF 1934 Sec. 13

(A)

*Make and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the issuer;*

(B)

devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that—

<http://www.sec.gov/>



COSO IS The Chosen Framework By Most Public Companies

# SEC Requirements Cont.

**(i) transactions are executed in accordance with management's general or specific authorization;**

(ii) transactions are recorded as necessary (I) to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements, and (II) to maintain accountability for assets;

(iii) access to assets is permitted only in accordance with management's general or specific authorization; and

(iv) the recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences

This Act identifies and prohibits certain types of conduct in the markets and provides the Commission with disciplinary powers over regulated entities and persons associated with them <http://www.sec.gov/about/laws/sea34.pdf>.

**Not Just About Accounting But About Authorization and Accountability**

# SEC Control Exception

## El Paso's Failure Properly to Account for Its Purchases of Iraqi Crude Oil

32. El Paso's accounting for its Oil for Food transactions failed properly to record the nature of the company's payments. In at least fifteen transactions, a portion of the company's purchase price for Iraqi crude oil constituted surcharge payments to Iraq in **violation of U.N. regulations and U.S. and international trade sanctions**. The company failed to so designate those payments, characterizing them instead simply as part of El Paso's cost of goods sold. Thus, El Paso failed to accurately record these payments in its books, records, and accounts.

### CLAIMS FOR RELIEF

#### FIRST CLAIM

[Violations of Section 13(b)(2)(A) of the Exchange Act]

33. Paragraphs 1 through 32 are realleged and incorporated by reference.

34. As described above, El Paso, through its officers, agents and subsidiaries, failed to keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflected its transactions and dispositions of its assets.

35. By reason of the foregoing, El Paso violated Section 13(b)(2)(A) of the Exchange Act [15 U.S.C. § 78m(b)(2)(A)].

#### SECOND CLAIM

[Violations of Section 13(b)(2)(B) of the Exchange Act]

36. Paragraphs 1 through 35 are realleged and incorporated by reference.

37. As described above, with respect to illegal surcharge payments made in connection with El Paso's purchases of Iraqi crude oil, **El Paso failed to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that: (i) payments were made in accordance with management's general or specific authorization; and (ii) payments were recorded as necessary to maintain accountability for its assets.**

38. By reason of the foregoing, El Paso violated Section 13(b)(2)(B) of the Exchange Act [15 U.S.C. § 78m(b)(2)(B)]. 11

Holding Companies Accountable for Violating a Regulations

# SEC Control Exception

## **El Paso's Failure Properly to Account for Its Purchases of Iraqi Crude Oil**

- Violation of U.N. regulations and U.S. and international trade sanctions
- Failed to so designate payments correctly (should not have been cost of goods sold)

[Violations of Section 13(b)(2)(A) of the Exchange Act]

- Failed to keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflected its transactions and dispositions of its assets.
- illegal surcharge payments made in connection with El Paso's purchases of Iraqi crude oil

**El Paso failed to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that:**

- (i) payments were made in accordance with management's general or specific authorization; and
- (ii) payments were recorded as necessary to maintain accountability for its assets.

38. By reason of the foregoing, El Paso violated Section 13(b)(2)(B) of the Exchange Act [15 U.S.C. § 78m(b)(2)(B)]. 11  
<https://www.sec.gov/litigation/litreleases/2007/lr19991.htm>

**Holding Companies Accountable for Violating Regulations**

# Consequences of an SEC Violation

## Scientific Industries CEO and Controller held accountable

Conspired to falsely inflate ESI's declining financial results by covering up significant expenses through various accounting devices

### PRAYER FOR RELIEF

WHEREFORE, the Commission respectfully requests that the Court:

1. **Permanently enjoin** Dooley and his agents, servants, employees, attorneys, and all persons in active concert or participation with them who receive actual notice of the judgment by personal service or otherwise from directly or indirectly violating, or aiding and abetting violations of, Section 17(a) of the Securities Act, Sections 10(b), 13(a), 13(b)(2)(A), 13(b)(2)(B), and 13(b)(5) of the Exchange Act, and Rules 10b-5, 12b-20, 13a-13, 13a-14, 13b2-1, and 13b2-2 thereunder;
2. **Permanently** enjoin Defendants **from serving as an officer or director** of any entity having a class of securities registered with the Commission pursuant to Section 12 of the Exchange Act [15 U.S.C. § 78j] or that is required to file reports pursuant to Section 15(d) of the Exchange Act [15 U.S.C. § 78o(d)];
3. Order Defendants to **disgorge all** wrongfully obtained **benefits, plus** prejudgment **interest**;
4. Order Defendants to **pay civil penalties** under Section 20(d) of the Securities Act [15 U.S.C. § 77t(d)] and Section 21(d) of the Exchange Act [15 U.S.C. § 78u(d)];
5. Retain jurisdiction of this action in accordance with the principles of equity and the Federal Rules of Civil Procedure in order to implement and carry out the terms of all orders and decrees that may be entered, or to entertain any suitable application or motion for additional relief within the jurisdiction of this Court; and

<https://www.sec.gov/litigation/litreleases/lr18896.htm>

Holding Officers and Others Accountable

# Consequences of an SEC Violation

## Long-term repercussions from SEC actions:

1. Permanently enjoin from not being in compliance with regulation
2. Permanently enjoin Defendants from serving as an officer or director of any public entity
3. Disgorge all wrongfully obtained benefits, plus prejudgment interest;
4. Pay civil penalties

Licenses and certifications are at risk

Continued employment in US unlikely

<http://www.sec.gov/divisions/enforce/friactions.shtml>

## Internal audit functions can be called into question

- ▶ Finally, Dutchmen lacked an effective internal audit function. The internal auditor Dutchmen hired in 2005 had little understanding of required internal control testing and, in fact, performed few internal audit functions. She also reported directly to Schwarzhoff, not to Thor's Internal Audit function. Moreover, Thor Internal Audit provided limited review of internal controls at Dutchmen, and indeed at other Thor subsidiaries. Thor Internal Audit was understaffed; performed a limited number of audits; failed to provide robust assessment of segregation of duties; and had inadequate procedures to validate supporting evidence Schwartzhoff submitted during control testing.

<http://www.sec.gov/litigation/complaints/2011/comp21966.pdf>

Another example of Internal Audit Failure

<http://www.sec.gov/litigation/complaints/2012/comp22306.pdf>

## Whistleblower laws increase potential for more actions

- ▶ *Washington D.C., April 22, 2015* — The Securities and Exchange Commission today announced an award of more than a million dollars to a ***compliance professional*** who provided information that assisted the SEC in an enforcement action against the whistleblower's company.

Holding Officers and Others Accountable

# Other SEC Actions Against Contractors

[SEC.gov | SEC Charges Oregon-Based Defense Contractor ...](#)

[www.sec.gov/.../2015-62.html](http://www.sec.gov/.../2015-62.html) U.S. Securities and Exchange Commission

- *Washington D.C., April 8, 2015* — The Securities and Exchange Commission today charged Oregon-based FLIR Systems Inc. with violating the Foreign Corrupt Practices Act (FCPA) by financing what an employee termed a “world tour” of personal travel for government officials in the Middle East who played key roles in decisions to purchase FLIR products. FLIR earned more than \$7 million in profits from sales influenced by the improper travel and gifts.

<http://www.insidegovernmentcontracts.com/2015/04/sec-and-state-oig-allege-that-contractors-policies-procedures-and-agreements-suppress-whistleblowing/>

- SEC and State OIG Allege that Contractors’ Policies, Procedures, and Agreements Suppress Whistleblowing  
By [Saurabh Anand](#) and [Susan Cassidy](#) on April 8th, 2015 Posted in [Defense Industry](#), [False Claims Act](#), [Government Contracts Regulatory Compliance](#), [Procurement Fraud and Internal Investigations](#) In a span of two days, two separate agencies took action against contractor policies and agreements that may discourage whistleblowers. On March 30, 2015, the U.S. Department of State Office of Inspector General (“State OIG”) issued [a report](#) contending that certain contractor policies and agreements have a “chilling effect” on whistleblowers. On April 1, 2015, the Securities and Exchange Commission (“SEC”) [imposed a fine](#) of \$130,000 on a contractor for requiring confidentiality agreements that allegedly impede individuals from disclosing securities law violations. Given recent scrutiny, contractors should consider reviewing policies, procedures, forms, agreements, or practices that may impede employees’ ability to report instances of fraud, waste, and abuse.

Accountability for Laws and Regulations

# Government Adoption of Similar Requirements

## A. Background

In **1982**, Congress enacted the ***Federal Managers' Financial Integrity Act*** (FMFIA), which requires each agency to establish and maintain internal control systems that allow:

- obligations and costs to be recorded in compliance with applicable laws;
- funds, property, and other assets to be safeguarded; and
- revenues and expenditures applicable to agency operations to be properly recorded and accounted for to permit the preparation of accounts and reliable financial information and statistical reports and to maintain accountability over the assets.

Following the publication of the initial GAO Standards, the Office of Management and Budget (OMB) issued Circular A-123 to provide specific guidance for agencies to follow in implementing internal control programs. In **1995**, OMB **revised** Circular **A-123** to require internal controls to support the purpose of the newly enacted *Government Performance and Results Act of 1993*, namely the improvement of program effectiveness and accountability. This revision required agencies to transmit a single annual Statement of **Assurance** from the head of the agency to the President, Congress, and OMB, stating whether there is reasonable assurance that the agency's **controls are achieving intended objectives.**

# Similar to SEC Requirements

## ***Federal Managers' Financial Integrity Act***

- ▶ Accuracy of books and records in accordance to laws and regulations
- ▶ Assets safeguarded
- ▶ Perform accountability of assets
- ▶ Assurance by management that controls are achieving objectives
  - OMB Circular A-123, Managements Responsibility for Internal Control
    - This Circular emphasizes the need for integrated and coordinated internal control assessments that synchronize all internal control-related activities
    - [https://www.whitehouse.gov/omb/circulars\\_a123\\_rev](https://www.whitehouse.gov/omb/circulars_a123_rev)

***A-123 Similar to COSO Objectives***

# Audit and Contractor Responsibilities

Management controls are required under DEAR 970-5203-1 which is incorporated in most Prime Contracts

- (a)(I) The **contractor** shall be **responsible** for maintaining, as an integral part of its organization, **effective systems of management controls** for both administrative and programmatic activities. Management controls comprise the plan of organization, methods, and procedures adopted by management to reasonably ensure that: the mission and activities assigned to the contractor are properly executed; efficient and effective operations are promoted; resources are safeguarded against waste, loss, mismanagement, unauthorized use, or misappropriation; all encumbrances and costs that are incurred under the contract and fees that are earned are in compliance with applicable clauses and other current terms, conditions, and intended purposes; all collections accruing to the contractor in connection with the work under this contract, expenditures, and all other transactions and assets are properly recorded, managed, and reported; and financial, statistical, and other reports necessary to maintain accountability and managerial control are accurate, reliable, and timely.
- (2) The **systems of controls** employed by the contractor shall be **documented** and satisfactory to DOE.
- (3) Such systems shall be an integral part of the contractor's management activities, including defining specific roles and responsibilities for each level of management, and holding employees accountable for the adequacy of the management systems and controls in their areas of assigned responsibility.
- (4) The contractor shall, as part of the **internal audit** program required elsewhere in this contract, periodically **review** the management systems and **controls** employed in programs and administrative areas **to ensure** that they are **adequate** to provide reasonable assurance that the objectives of the systems are being accomplished and that these systems and controls are **working effectively**. Annually, or at other intervals directed by the contracting officer, the contractor shall supply to the contracting officer copies of the reports reflecting the status of recommendations that result from audits of business, financial, or management controls performed by its internal audit activity and any other audit activity.
- (b) The contractor shall be responsible for maintaining, as a part of its operational responsibilities, a baseline quality assurance program that implements documented performance, quality standards, and control and assessment techniques.

# Contract Clauses

## 48 CFR 970.5203-1 - Management controls

1. Maintain a system of controls to ensure:
  - Mission and function are properly executed
  - Efficient and effective operations
  - Resources are safeguarded
  - Costs are according to contract, laws and regulations
  - Expenditure, transaction and assets are reported accurately and properly managed
  - Management monitoring for accountability
2. Satisfactory system of controls
3. Defined management roles and responsibilities
4. Perform periodic management assessments/audits and report annually (i.e. or according to CO)
  - Controls are Adequate (i.e. designed appropriately)
  - Controls are working effectively (i.e. operating as designed)
5. Maintain a quality assurance program

Requirements Contain Similar Themes



© 1992-2013, The Committee of Sponsoring Organizations of the Treadway Commission (COSO), All rights reserved. Used with permission.

# Department of Justice Collects \$\$



## Boeing Legal Issues 2002-2005

- Boeing is the one of the nation's biggest military contractors. It is under fire for unethical handling of Pentagon contracts and trade secrets
  - Officers indicted, penalties assessed and careers ended
  - Boeing paid a total of **\$615 million** dollars to resolve the government's investigations and claims
- James McNerney takes over as CEO

“I believe that American companies are in an analogous position today with ethics and compliance. We have to get everyone involved in taking responsibility for ethics and compliance. More than that, we need to make the **leap from defense to offense** . . . in thinking of **ethics and compliance** as part of the leadership agenda and as a powerful discriminator between companies-  
-indeed, for the best companies, a real source of **competitive advantage**.”



Emphasis on better accountability and controls

# The Law Department at Boeing

The Law department is responsible for the delivery of all legal services for Boeing throughout the world. In addition to the Corporate Offices Group, the General Counsel's Office includes legal staff at each of Boeing's operating segments.

- ▶ In May 2006, then-Judge J. Michael Luttig- made major news in the legal world by resigning from the U.S. Court of Appeals for the Fourth Circuit to become senior vice president and general counsel of aerospace giant Boeing. Luttig served as a Fourth Circuit judge for almost 15 years, during which time he reigned as the #1 feeder judge, sending almost all of his clerks into Supreme Court clerkships, and came extremely close to becoming a justice himself.
- ▶ Boeing boasts at least eight (8) US Supreme Court clerks
  - John Demers (OT 2005/Scalia), Grant Dixton (OT 2000/Kennedy), Brett Gerry (OT 2000/Kennedy), and Jake Phillips (OT 2004/Scalia), Bertrand-Marc Allen (OT 2003/Kennedy), Lynda Guild Simpson (OT 1984/Powell), and Eric Wolff (OT 2000/Scalia)..

In addition to all legal services:

- ▶ Compliance to the foreign corrupt practices act
  - Functional process owner
  - Annual risk assessment
- ▶ Oversight of higher risk subsidiaries
- ▶ Supports Ethics and Corporate investigations

**Restructured To Address Compliance Risks**

# Excerpt /Federal Sentencing Guidelines

## Federal Sentencing of Organizations

*This chapter is designed so that the sanctions imposed upon organizations and their agents, taken together, will provide just punishment, adequate deterrence, and incentives for organizations to maintain internal mechanisms for preventing, detecting, and reporting criminal conduct.*

### **Generally are vicariously liable for offenses committed by their agents**

*Federal prosecutions of organizations therefore frequently involve individual and organizational co-defendants*

*j) An individual was "willfully ignorant of the offense" if the individual did not investigate the possible occurrence of unlawful conduct despite knowledge of circumstances that would lead a reasonable person to investigate whether unlawful conduct had occurred.*

D) Apply §8C2.5 (Culpability Score) to determine the culpability score. To determine whether the organization had an effective compliance and ethics program for purposes of §8C2.5(f), apply §8B2.1 (Effective Compliance and Ethics Program).

**The two factors that mitigate the ultimate punishment of an organization are: (i) the existence of an effective compliance and ethics program; and (ii) self-reporting, cooperation, or acceptance of responsibility.**

**Must Meet Objectives to Play Offense**

# \* DOJ Assistant Attorney General Leslie Caldwell

## Nine Key Attributes for Which Companies Should:

1. **High-level commitment** - ensure that its directors and senior management provide strong, explicit, and visible commitment to its corporate compliance policy.
2. **Written Policies** - have a clearly articulated and visible corporate compliance policy memorialized in a written compliance code.
3. **Periodic Risk-Based Review** - periodically evaluate these compliance codes on the basis of a risk assessment addressing the individual circumstances of the company.
4. **Proper Oversight and Independence** - assign responsibility to senior executives for the implementation and oversight of the compliance program.
5. **Training and Guidance** - implement mechanisms designed to ensure that its compliance code is effectively communicated to all directors, officers, employees.
6. **Internal Reporting**- have an effective system for confidential, internal reporting of compliance violations.
7. **Enforcement and Discipline** - implement mechanisms designed to enforce its compliance code, including appropriately incentivizing compliance and disciplining violations.
8. **Third-Party Relationships** - institute compliance requirements pertaining to the oversight of all agents and business partners.
9. **Monitoring and Testing** - conduct periodic reviews and testing of its compliance code to improve its effectiveness in preventing and detecting violations.

Audit Support Through Testing or Advisory

\* 22nd Annual Ethics and Compliance Conference Oct. 1, 2014

# Department Of Justice

Stuart F. Delery, Principal Deputy Assistant Attorney General for the Civil Division of the Department of Justice, said: "**Contractors owe a duty to the taxpayers to accurately bill the United States for work performed**".

"**Vigorously prosecuting financial fraud is one of the Justice Department's top priorities,**" said Assistant Attorney General Tony West.

## **Culpability is weighted by a number of factors:**

- ▶ When criminal misconduct is discovered, a critical factor in the department's prosecutorial decision making is the **extent and nature of the company's cooperation**.
- ▶ The department's Principles of Federal Prosecution of Business Organizations provides that prosecutors should consider "the corporation's **timely and voluntary disclosure** of wrongdoing and its **willingness to cooperate** in the investigation of its agents."
- ▶ Additionally, for a company to receive full cooperation credit, the company must **provide relevant documents and evidence**, and should do so in a timely fashion.
- ▶ But for a company to receive credit for its compliance program, it must have demonstrated effectiveness, with **messages about compliance that come from the top** and echo throughout the corporate hallways.
- ▶ And for a company to receive full cooperation credit, it **must uncover the misconduct, identify the responsible individuals, and fully disclose the facts to the department.**

# Ethics & Compliance

## Vision:

A culture where ethical behaviors and adherence to compliance objectives are expected, understood and upheld (provides a competitive advantage).

## Mission:

Create and oversee an ethics and compliance program that drives business success through positive change and personal accountability.

Develop A Strategy To Achieve The Mission

# Ethics & Compliance



## Company Requirements and Responsibilities:

- ▶ All managers are responsible to ensure effective compliance controls exist
- ▶ No less than annual compliance risk status assessments
- ▶ A defined set of criteria for identifying, measuring, evaluating, monitoring, and reporting compliance risk within the organization or function
- ▶ Appropriate assignment of authority vesting in executive leadership over compliance risk areas
- ▶ A compliance monitoring program appropriate to the size of the organization
- ▶ Appropriate compliance training be made available to employees as needed
- ▶ Measurement of the effectiveness of internal controls
- ▶ Periodic compliance audits
- ▶ Appropriate delegation of authority for compliance matters
- ▶ Continued monitoring of critical risks



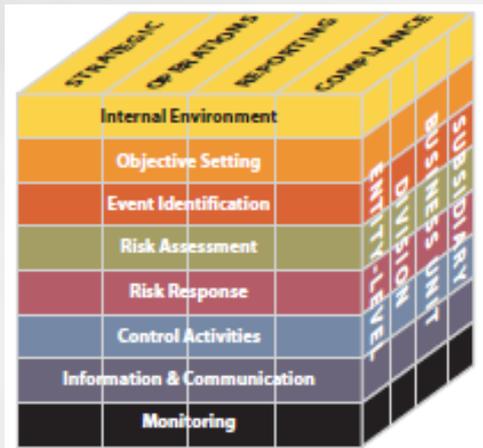
(Notional) Compliance Risk Program and Strategic Roadmap (May 2015)

COMPONENT	YEAR 1	YEAR 2	YEAR 3	YEAR 4
ETHICS AND COMPLIANCE RISK MANAGEMENT	<ul style="list-style-type: none"> <li>Identify and engage subject matter experts to surface key risks across the firm.</li> <li>Conduct a gap analysis to understand firm-wide compliance and legal risks and current control gaps:               <ul style="list-style-type: none"> <li>Develop an initial list of core risks to review.</li> <li>Involve a small cross-functional group to assess and prioritize core risks.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Convene subject matter experts across the organization to assess key risks.</li> <li>Document company and industry-specific legal and regulatory requirements.</li> <li>Create uniform criteria to assess legal and compliance risks across likelihood and severity.</li> </ul>	<ul style="list-style-type: none"> <li>Survey organizations and functions regularly to uncover changes in compliance risk exposures.</li> <li>Update potential list of risk exposures with (potential) changes to legal and regulatory landscape.</li> <li>Facilitate business unit-owned risk self-assessments that roll up to the corporate center.</li> <li>Work with the business to develop risk mitigation plans.</li> </ul>	<ul style="list-style-type: none"> <li><u>Integrate</u> compliance risk assessments with enterprise-wide risk detection efforts.</li> <li>Develop detailed <u>risk-specific</u> (e.g., EH&amp;S, data privacy) compliance <u>standards</u> for business units.</li> <li><u>Align</u> organizational and functional unit-owned risk self-assessments and mitigation plans with strategic business plans.</li> <li>Use an employee survey to understand core culture, employee perceptions, and related risks.</li> </ul>
	<p><b>Key Metrics / Milestones:</b></p> <ul style="list-style-type: none"> <li>Identification of top 5 corporate compliance risks</li> </ul>	<p><b>Key Metrics / Milestones:</b></p> <ul style="list-style-type: none"> <li>Documentation and assessment of most significant compliance and legal risks to company</li> <li>Number of compliance control issues documented in internal audit reports</li> </ul>	<p><b>Key Metrics / Milestones:</b></p> <ul style="list-style-type: none"> <li>Identification of top 5 corporate compliance risks to company (by location, business unit)</li> <li>Percent of major business units completing risk assessment</li> <li>Progress against risk mitigation plans</li> </ul>	<p><b>Key Metrics / Milestones:</b></p> <ul style="list-style-type: none"> <li>Identification of top 5 compliance risks to company <u>Year-over-year changes</u> in organizational or functional risk assessment results</li> <li>Number of citations issued by regulatory agencies</li> <li>Internal audit compliance-testing results</li> </ul>

# Next Steps

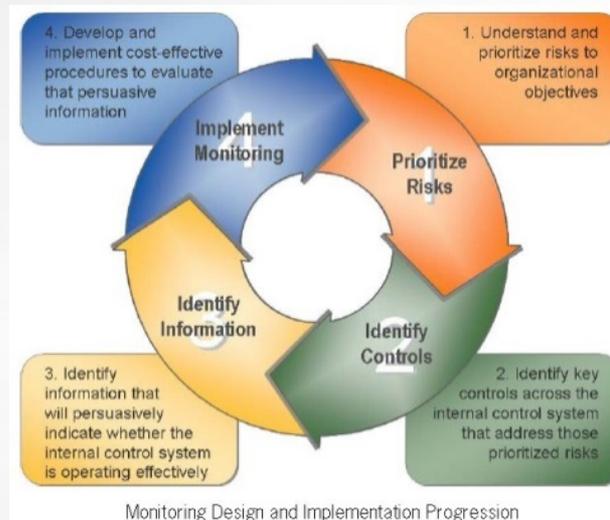
- Identify the key assertions/objectives
- Find the underlying procedures
- Assess the risks
- Evaluate the design and effectiveness of controls

2004



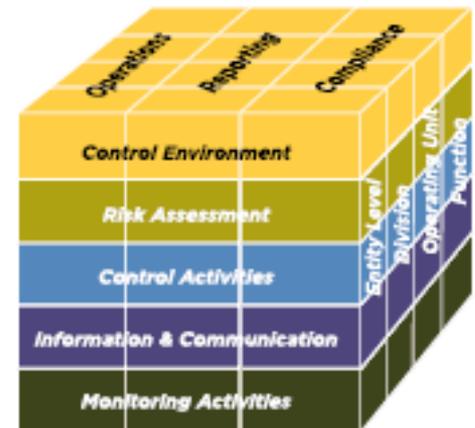
© 1992-2013, The Committee of Sponsoring Organizations of the Treadway Commission (COSO), All rights reserved. Used with permission.

2009



Monitoring Design and Implementation Progression

2013



© 1992-2013, The Committee of Sponsoring Organizations of the Treadway Commission (COSO), All rights reserved. Used with permission.

# Management Assertions

\*as·ser·tion  
ə'sərSH(ə)n/

noun:

**assertion**; plural noun: **assertions**

a confident and forceful statement of fact or belief.

"his **assertion that** his father had deserted the family

synonyms:

declaration, contention, statement, claim, opinion, proclamation, announcement, pronouncement, protestation, avowal;

The action of stating something or exercising authority confidently and forcefully.

"the assertion of his legal rights"

synonyms:

defense of, upholding of; insistence on

"an **assertion of the right to march**"

\*[https://www.google.com/?gws\\_rd=ssl#q=Definition+of+assertion](https://www.google.com/?gws_rd=ssl#q=Definition+of+assertion)

---

November 1, 2014 Federal Sentencing Guidelines Manual **§8B2.1**

Compliance Assertions:

- Risks Are Identified
- Controls Effectively Mitigate Risks
- Ensure Objectives Are Met

# Function = Financial Reporting

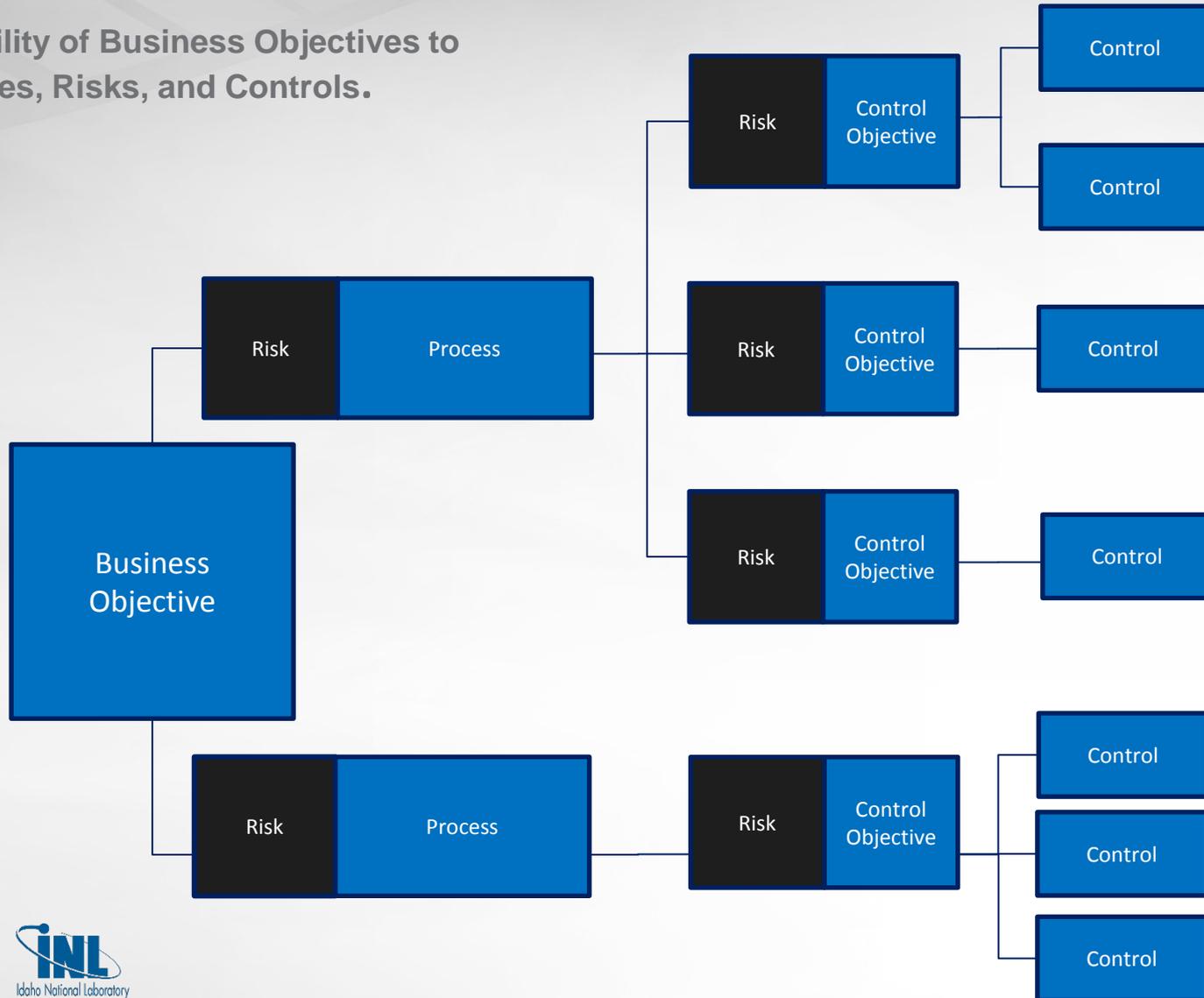
Internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting. Reliability of financial reporting means that management can reasonably make the following **assertions**:

- ▶ All reported transactions actually occurred during the reporting period and all assets and liabilities exist as of the reporting date (existence and occurrence);
- ▶ All assets, liabilities, and transactions that should be reported have been included and no unauthorized transactions or balances are included (completeness);
- ▶ All assets are legally owned by the agency and all liabilities are legal obligations of the agency (rights and obligations);
- ▶ All assets and liabilities have been properly valued, and where applicable, all costs have been properly allocated (valuation);
- ▶ The financial report is presented in the proper form and any required disclosures are present (presentation and disclosure);
- ▶ The transactions are in compliance with applicable laws and regulations (compliance);
- ▶ All assets have been safeguarded against fraud and abuse; and
- ▶ Documentation for internal control, all transactions, and other significant events is readily available for examination.

There Are Multiple Functions Which Assert To Laws and Regulations

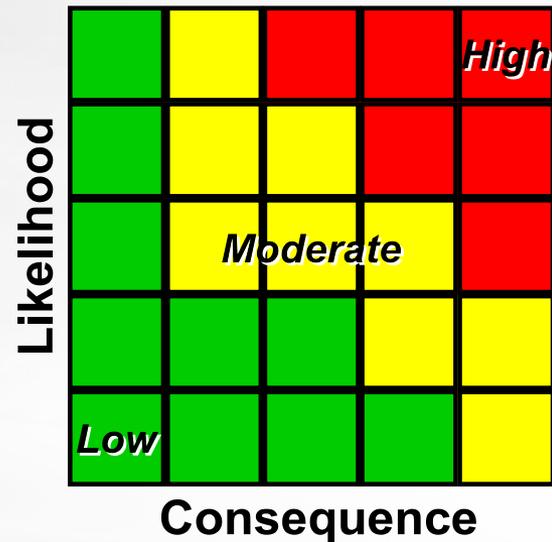
# Line of Sight

- Traceability of Business Objectives to Processes, Risks, and Controls.



# Risk Definition

- The possibility that an event will occur and adversely affect the achievement of business objectives
- Risk events consists of two components:
  - Likelihood: The possibility an event will occur
  - Consequence: The result or effect of an event



***Identify and document the "Risk Event"***

# Example- Risk – Related to State or Federal Tax returns

## Consequence

## Risk Events?

### Fines and Penalties

- Missing the deadline to submit timely state tax returns may result in fines and penalties

### Damage to company image or reputation

- Missing the deadline to submit timely state tax returns may damage company image or reputation in the business community

### Incurring additional costs to support an increase in frequency of state audits

- Continually missing the deadline to submit timely state tax return may result in an increase in state audit frequency creating additional support costs

What might be some lower level risk events?



## Conditional Probability

The probability that event A occurs given that event B has already occurred is called the conditional probability of A given B. Symbolically, this is written as  $P(A|B)$ . The probability it rains on Monday given that it rained on Sunday would be written as  $P(\text{Rain on Monday} | \text{Rain on Sunday})$ .

# Working Down The Risk Hierarchies

## **Missing the deadline to submit timely state tax returns may result in fines and penalties**

- Determine what the key events are and to what extent they should be mitigated

	<b>Risk #</b>	<b>Risk Description</b>
	1	Approval signatures are not available in a timely manner
	2	The payment process takes too long Approvals/signatures are not available until xx Bank processing takes 10 days after approval to deliver payment
	3	The sales activity for the period is not available in a timely manner resulting in returns not being completed timely

**Key Events** are those events that are prioritized as more likely to occur and cause a condition that would lead to the realization of a consequence.

# Risk/Control Mapping

Risk #	Control Description	Control Type		
		Preventive	Detective	Monitoring
1	State revenue tax return approvers are scheduled to review and approve returns during the 10th through the 15th of each month - A list of approves is maintained with backups identified in an available database-Completion of scheduled review tracked	X		
2	Tax return completions are tracked within a database program which notifies management when a scheduled tax return has not been approved within the designated time period		X	
3	Fines and penalties accounts are monitored for activity by the appropriate accounting manager – Corrective actions taken			X

# Testing Results

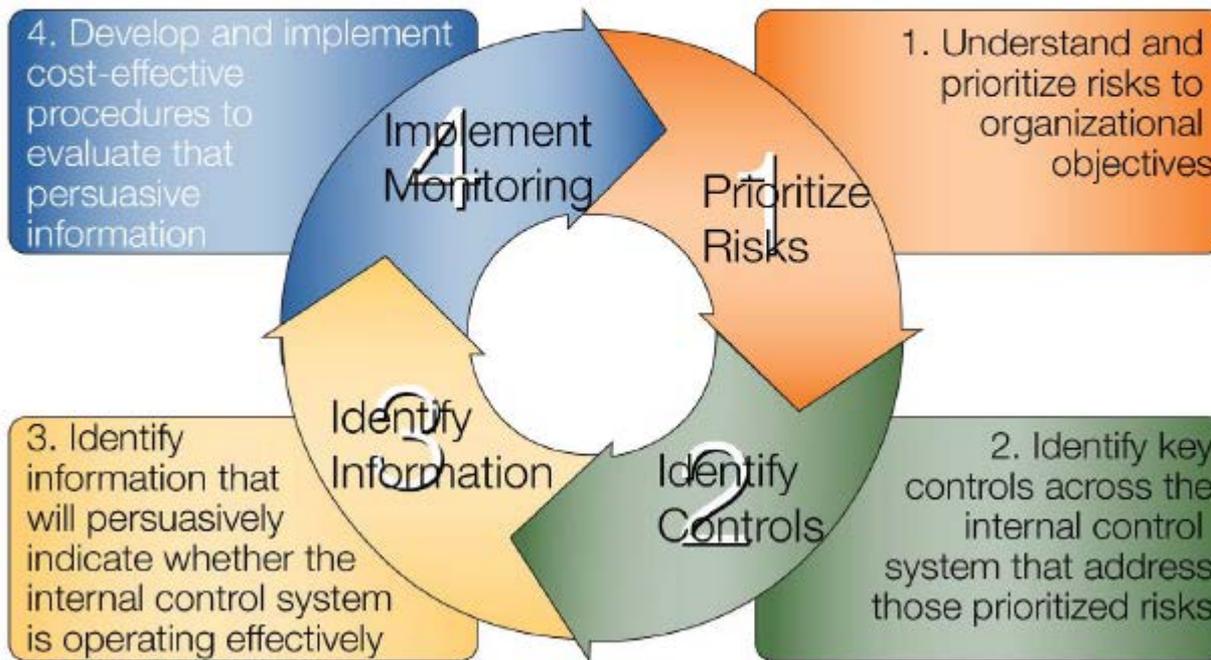
Risk #	Control Description	Control Type			Control Design Review		
		Preventive	Detective	Monitoring	Design Issue	Effective	Ineffective

- A deficiency in design exists when:
  - A control necessary to meet the control objective is missing; or
  - An existing control is not properly designed so that, even if it operates as designed, the control objective is not always met.
- A deficiency in operation exists when:
  - A properly designed control does not operate as designed; or
  - When the person performing the control does not possess the necessary authority or qualifications to perform the control effectively.

**Significant Deficiency** – a deficiency, or combination of deficiencies, that results in more than a remote likelihood that a targeted event will not be prevented or detected leading to a high probability of experiencing a prioritized risk.

# Continuous Improvement of Internal Controls

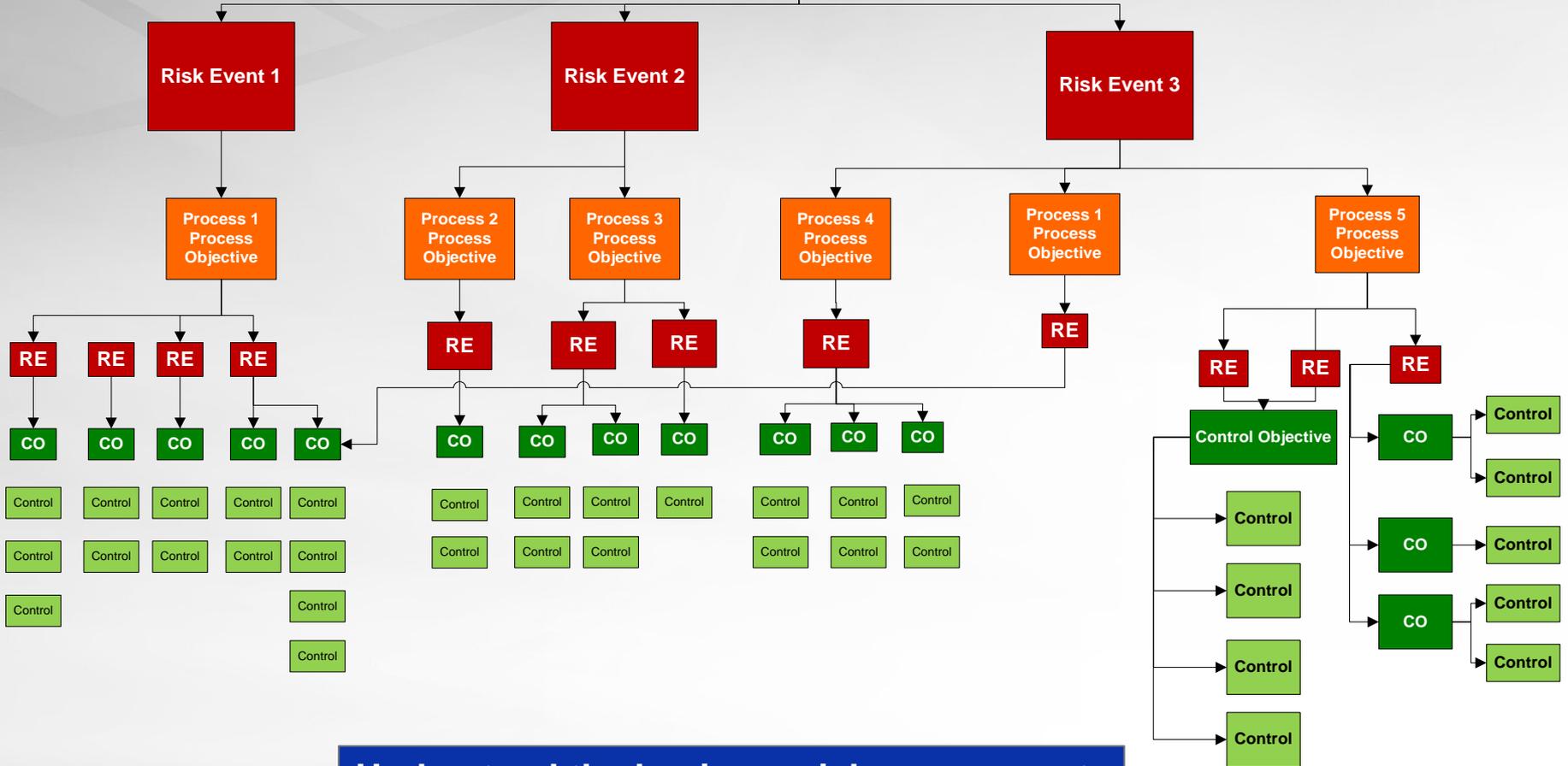
## Monitoring Design & Implementation Progression



Copyright © 2013 Boeing. All rights reserved.

3033

# Business Objective



Understand the business risk assessment

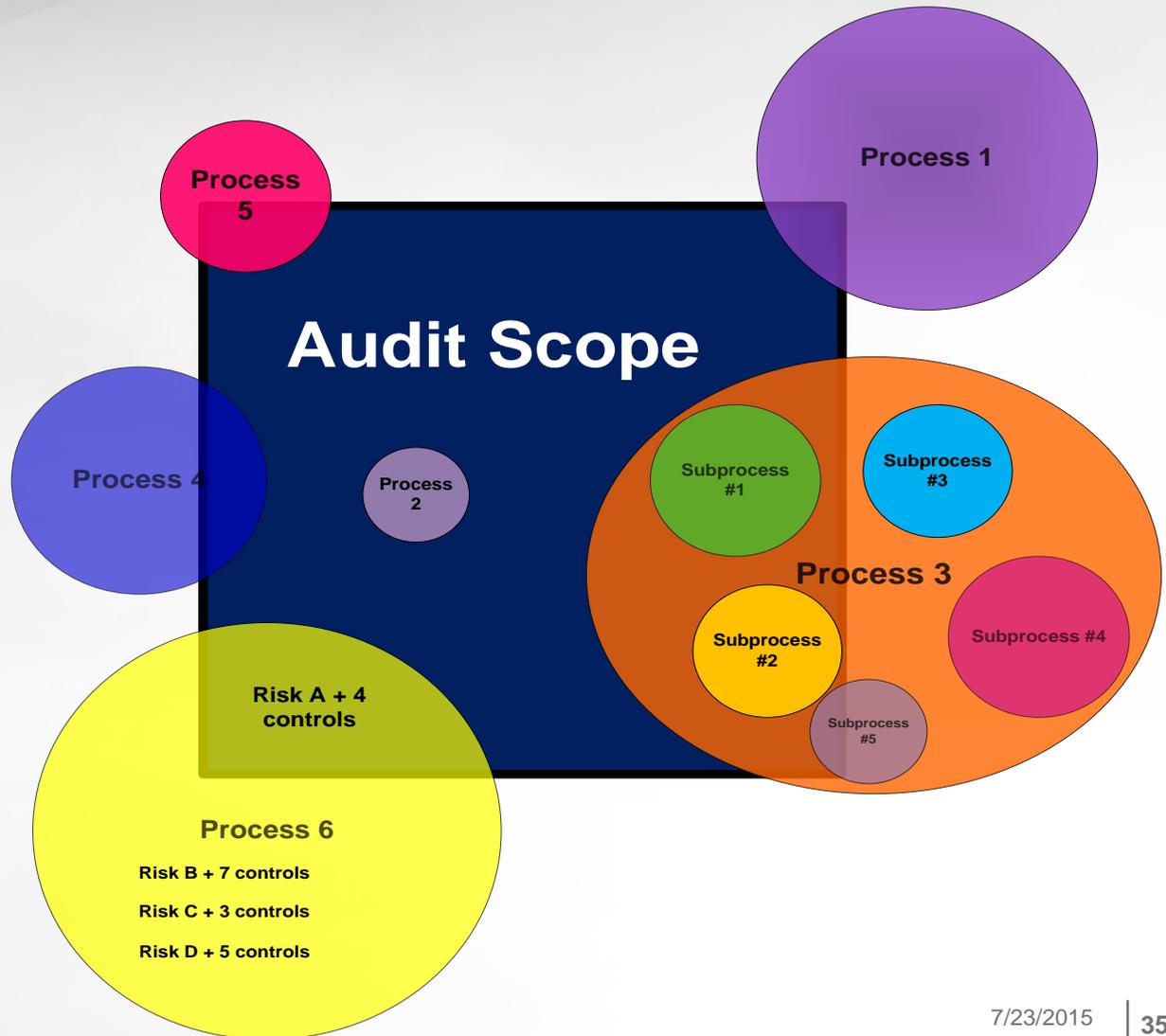
# Audit Scope Pictorial

Client responses and data referenced during Risk Assessment typically describe “risks” in terms of escapes, conditions and problems.

How do we determine the **appropriate boundaries** of the audit scope?

How do we **determine the processes** to bring into scope?

How do we align the **the scope of the audit** to ensure coverage of the highest risk areas?



# Scoping Considerations

- ▶ How do we determine the appropriate boundaries for the scope of the audit?
- ▶ How do we determine what processes to bring into scope?
- ▶ How do we align the scope of the audit to ensure coverage of the highest risk areas?

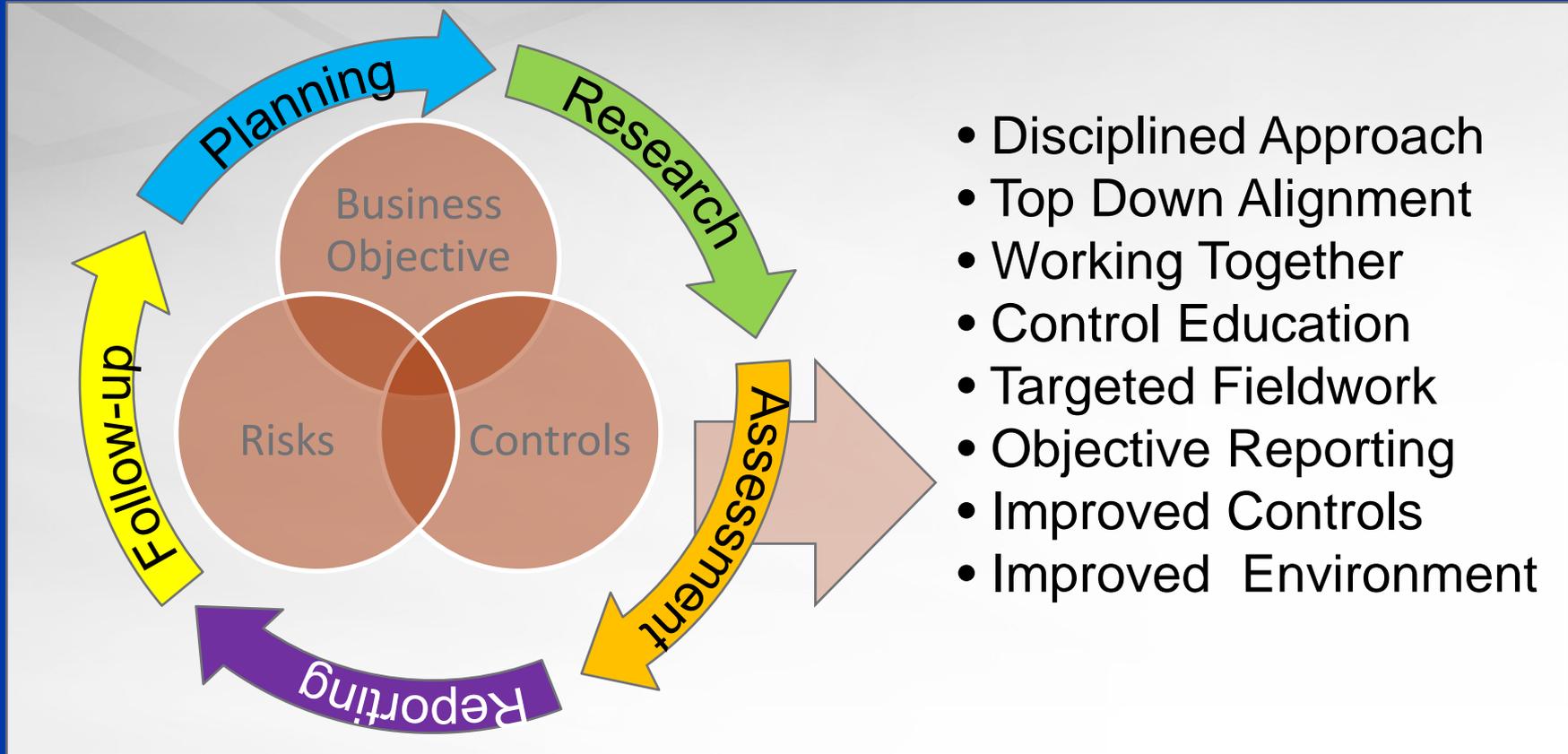
Understanding the objectives and underlying Risk Events

Understanding where the Controls reside that would mitigate the Risk Events

Understanding the relative strength of the controls that mitigate the Risk Events

# Audit Model

## Control Activities



- Disciplined Approach
- Top Down Alignment
- Working Together
- Control Education
- Targeted Fieldwork
- Objective Reporting
- Improved Controls
- Improved Environment

Information & Communications

Risk Assessment