COSO: The Ultimate Contract Compliance Tool

March 2016

TABLE OF CONTENTS

CLASS TAKE-AWAYS

- Understand what the COSO framework is
- Practical understanding of how to apply COSO to **U.S. Government contract compliance**
- Ability to create a common dialogue about contract compliance across an organization

Who is COSO?

- **Committee of Sponsoring Organizations of the Treadway Commission (COSO)** - a joint initiative of five private sector organizations dedicated to providing thought leadership to executive management and governance entities on critical aspects internal control
- Five (5) private sector organizations are:
  - Institute of Management Accountants (IMA)
  - American Accounting Association (AAA)
  - American Institute of Certified Public Accountants (AICPA)
  - Institute of Internal Auditors (IIA)
  - Financial Executives International (FEI)

WHAT IS COSO?

Why was COSO started?

- Originally, in response to questionable corporate political finance activities (Foreign Corrupt Practices Act) (1985)

- Later, leveraged by the public accounting industry in response to Sarbanes-Oxley (SOX 404) in response to Enron, and similar public investor fears of corporate fraud

What is the COSO Framework?

- An enterprise risk management tool founded on the use of internal controls for achieving reliable and responsible corporate objectives around:
  - Corporate strategy
  - Operations
  - Financial reporting; and
  - Compliance with rules and regulations

What is the COSO Framework?

- In basic terms:

"Investors needed more confidence that they weren't being ripped off by corporate { INSERT CURSE WORDS} so they created a solution."

"Then the Government got jealous of SOX and decided to copy/paste the requirements"

- Ryan Koenitzer, CPA – wildly unsuccessful screenwriter/baseball player ~~turned~~ forced into USG contract compliance professional

What is the COSO Framework?

- Who are the investors?

What is the COSO Framework?

Investors

- Shareholders
- Executive management
- Employees
- U.S. Government
- Taxpayers

COSO: Key Concepts

- Internal control - 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:
  - Effectiveness and efficiency of operations
  - Reliability of financial reporting
  - **Compliance with applicable laws and regulations.**
  - Safeguarding of Assets (MHA)

- Risk-based
  - The framework is based on identifying risks and linking them to key internal control activities

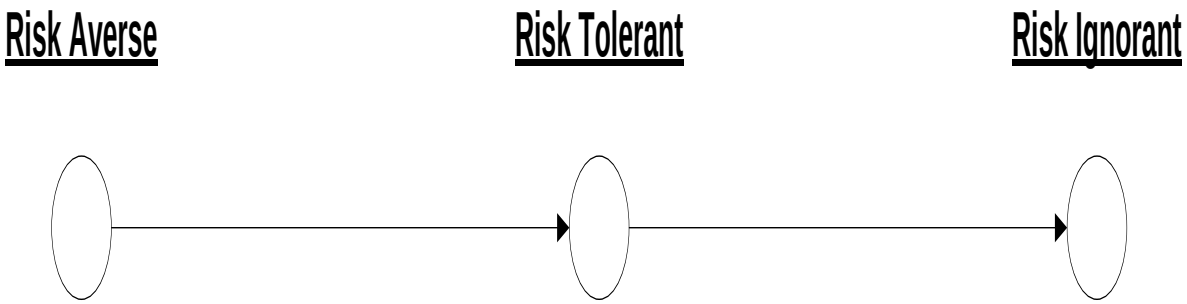
COSO: Key Concepts

Eight (8) key components of an effective internal control framework:

- Internal environment
- Objective setting
- Event identification
- Risk assessment
- Risk response
- Control activities
- Information and communication
- Monitoring

DEFINING RISK: Example Application

Every company, just like every individual, has a risk appetite:



Defining Risk: Example Application

Largely accomplished through a Risk Control Matrix (RCM), which maps key control activities to risks:

Process	Risk No.	Risk	Key Control No.	Key Control Activity	Control Owner

Defining Risk: Example Application

Example

Process	Risk No.	Risk	Key Control No.	Key Control Activity	Control Owner	Risk Culture
Parenting (3 Year Old)	R.01	Child falls out of "big boy" bed	C.01	Bedrails are installed on bed	Dad	Risk Tolerant
			C.01	Child sleeps in bed with you until he is fifteen (15) years old	Mom/Dad	Risk Averse
			C.01	Child sleeps on ground	Child Services	Risk Idiocy (My Brother)
			C.01	No control	N/A	Risk Averse

DEFINING RISK: U.S. Government Compliance

- U.S. Government compliance risks are broad and wide-encompassing
- Examples:
  - Labor charging
  - Cost/pricing
  - Billing
  - Ethical behavior
  - Procurement
  - Supplier monitoring
  - Government Property

DEFINING RISK: U.S. Government Compliance

- What is the best way to define risk in U.S. Government compliance?
- Recommendations:
  - Terms and conditions
  - Applicable rules and regulations
  - DCAA Audit Programs
  - DCAA Audit Reports
  - MRDs

- All of these things define, and help shape, the culture of risk at an organization

USG COMPLIANCE: Example Application

EXAMPLE:

Process	Term/Condition	Requirement	Risk No.	Risk	Key Control No.	Key Control Activity	Control Owner
Estimating	252.215-7002 Cost Estimating System Requirements	(xiv) Provide procedures to update cost estimates and notify the Contracting Officer in a timely manner throughout the negotiation process.	R.01	Information that would affect negotiations is not monitored and disclosed to the Contracting Officer	E.01	A TINA Sweep is performed and documented via a TINA Sweep Checklist, acknowledging key elements of proposed cost have been reviewed for requisite disclosure	Cost Estimating Manager

USG Compliance: Example Application

- Defining risk and assigning key controls is an art, not a science
- Internal controls only offer “reasonable assurance”; not “absolute”
- The better your definition of risk and assignment of key control objectives, the better your probability of attaining “reasonable assurance”

USG Compliance: Example Application

ANOTHER EXAMPLE (POOR):

Process	Term/Condition	Requirement	Risk No.	Risk	Key Control No.	Key Control Activity	Control Owner
Estimating	252.215-7002 Cost Estimating System Requirements	(xv) Provide procedures that ensure subcontract prices are reasonable based on a documented review and analysis provided with the prime proposal, when practicable.	R.02	Cost/price analysis is not performed on suppliers	E.01	Cost/price analysis is performed	Procurement Representative

USG Compliance: Example Application

ANOTHER EXAMPLE (BETTER):

Process	Term/Condition	Requirement	Risk No.	Risk	Key Control No.	Key Control Activity	Control Owner
Estimating	252.215-7002 Cost Estimating System Requirements	(xv) Provide procedures that ensure subcontract prices are reasonable based on a documented review and analysis provided with the prime proposal, when practicable.	R.02	Price analysis is not performed on competitively sourced suppliers	E.01	Price Analysis is performed and documented via Form USG-10 on all suppliers and retained in the proposal file	Procurement Representative
			R.03	Cost analysis is not performed on negotiated suppliers > $750K	E.02	A cost analysis, including a supplier cost/analysis Form USG-11, is performed on all suppliers > $750K and retained in the proposal file	Procurement Representative
			R.04	An item does not meet commercial item definition	E.03	All commercial items include justifications documented on a Commercial Item Determination Form USG-12, and are included in the proposal file	Procurement Representative

USG COMPLIANCE: Example Application

- The internal control framework is a living, breathing document
- Can be used to address:
  - New terms and conditions
  - New events or findings

Example:

Process	Term/Condition	Requirement	Risk No.	Risk	Key Control No.	Key Control Activity	Control Owner
Estimating	DCAA Audit Report	Proposed prices are not monitored against actuals	R.02	Proposed prices are not monitored against actual costs	E.04	Actual costs are monitored against proposed prices for all contracts > $5M	Cost Estimating Manager

USG COMPLIANCE: Example Application

Class Example:

Process	Term/Condition	Requirement	Risk No.	Risk	Key Control No.	Key Control Activity	Control Owner
Purchasing	252.244-7001	(5) Establish and maintain adequate documentation to provide a complete and accurate history of purchase transactions to support vendors selected and prices paid;	R.01				
			R.02				

MONITORING OF USG COMPLIANCE

- The internal control framework facilitates entity-wide monitoring including:
  - Evaluation of internal control efficiency
- Identification of control attributes
  - Preventive vs. Detective
  - Manual vs. Automated
  - Preference for Preventive/Automated Controls ("super controls")

Process	Term/Condition	Requirement	Risk No.	Risk	Key Control No.	Key Control Activity	Control Owner	Preventive / Detective	Automated / Manual
Indirect Cost Rates	DCAA Audit Program (Accounting System)	Indirect cost rates are monitored	R.01	Indirect cost rates are not monitored	E.01	Indirect cost rates are calculated on a monthly basis	U.S. Government Accounting Manager	P	M

MONITORING OF USG COMPLIANCE

- Creating test plans for testing operating effectiveness of the internal control design
- Test plans are created to evaluate if responsible employees are complying with the designed internal control activities
- Results offer empirical, data-driven analysis for management consideration in evaluating:
  - Compliance culture
  - Personnel
  - Adequacy of internal control design
- Failure of internal control testing may mean a flaw in:
  - People
  - Process (e.g., internal control design)
  - Technology

THE CASE FOR COSO

- It creates a common dialogue across the organization
- It offers a practical framework for responding to new/emerging risks
- It provides internal audit and/or management an empirical and diagnostic platform
- It is widely adopted as “best practice” by leading defense contractors

THE CASE FOR COSO

Most Importantly – The U.S. Government Expects It!

- *"DCAA's audit guidance for examining internal controls is based on the guidance published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO)."* **(MRD 2003)**
- *"Contractor business systems and internal controls are the first line of defense against waste, fraud, and abuse. Weak control systems increase the risk of unallowable and unreasonable costs on Government contracts."* **(DFARS Business System Rule "Background")**
- Debarment official required the use of COSO internal control framework as an element of remediation at alleged False Claim Act violator

Q & A

Questions?

Contact Info

Ryan Koenitzer, CPA

RKI

U.S. Government Contracts Practice

rkoenitzer@rkiaccounting.com

(617) 413-5438