May 28, 2014

David Sidon, The Navis Group
Todd Desjardins, BerryDunn

GAIN CONTROL OF YOUR FDICIA/SOX

TODAY'S AGENDA

Part 1 - 9:00 to 10:15am

Introductions

Surveying the Room

Defining FDICIA SOX & COSO

Current best practice for FDICIA / SOX

The external audit firm's role

COSO's New Guidance *(from the COSO slide deck)*

Break

Part 2 – 10:30 to 11:45am

"Rolling COSO Forward"

How methodology changes / expands

A practical approach – mapping the 87 focus points with a renewed emphasis on the entity-level and risk objectives

PCAOB – what is their role?

Q & A

PRESENTATION MATERIALS

Via BerryDunn and The Navis Group (*through BASECAMPHQ.com*)

- Today's Slide Deck
- The Full COSO Outreach Deck
- PCAOB – Auditing Standard #5 – "An Audit of Internal Control over Financial Reporting that is Integrated with an Audit of Financial Statements"
- Rolling COSO Forward (*hand-out in PDF format*)

SMALL SAMPLE BASELINE SURVEY

Banks Creeping up on FDICIA?

Banks Subject to FDICIA?

Banks Subject to Sarbanes-Oxley?

Who "OWNS" FDICIA/SOX in your institution?
CFO - CONTROLLER - RISK - INTERNAL AUDIT

Who should own COSO?

Who "TESTS" FDICIA/SOX in your institution?
OWNERS - RISK - INTERNAL AUDIT - OUTSOURCED

SMALL SAMPLE BASELINE SURVEY – PART 2

Testing as separate “event” or embedded in IA schedule?

What’s the Rhythm? Quarterly – Annual – What about Month 12?

Excel/Word Based? Custom? Software Solution (e.g., WolfPAC)?

Scope - Separate Entity-Level, Technology & Process-Specific Controls?

How Tied to Financial Statements – GL Acct Numbers/Groupings? Other?

Number of Controls? If more than 125, let’s talk!

What’s your testing effort metric? (two - three hours per control per year?)

FDICIA VS. SOX VS. COSO – IMPORTANT DISTINCTIONS

CUTTING THROUGH THE FOG – COMPLIMENTS OF MR. DICKENS

"Fog everywhere. Fog up the river, where it flows among green aits and meadows; fog down the river, where it rolls defiled among the tiers of shipping and the waterside pollutions of a great (and dirty) city. Fog on the Essex marshes, fog on the Kentish heights. Fog creeping into the cabooses of collier-brigs; fog lying out on the yards, and hovering in the rigging of great ships; fog drooping on the gunwales of barges and small boats. Fog in the eyes and throats of ancient Greenwich pensioners, wheezing by the firesides of their wards; fog in the stem and bowl of the afternoon pipe of the wrathful skipper, down in his close cabin; fog cruelly pinching the toes and fingers of his shivering little 'prentice boy on deck. Chance people on the bridges peeping over the parapets into a nether sky of fog, with fog all round them, as if they were up in a balloon, and hanging in the misty clouds."

Paragraph #2 - Bleak House, by Charles Dickens

FDICIA VS. SOX VS. COSO – IMPORTANT DISTINCTIONS

FDICIA

FDICIA (the FDIC Improvement Act of 1991, as amended) in part, requires banks with assets exceeding $1 billion to assert that an internal control methodology is in place to assure the integrity of the annual audited financial statements, as well as the four quarterly Call Reports.

The “measurement” date for asset size is the fiscal year-end, necessitating compliance the following year.

FDICIA VS. SOX VS. COSO – IMPORTANT DISTINCTIONS

SOX

SOX (the Sarbanes-Oxley Act of 2002) is a non-industry specific compliance requirement for all SEC registrants (those filing Qs and Ks).

SOX was born of the Enron era. SOX roll-out and enforcement was troublesome nationwide, as the effective date and metrics for small versus large companies was regularly postponed and amended. Years passed. The “measure” for this compliance requirement is a market capitalization level of $75 million (i.e., when “accelerated filer” status is attained). The “measurement” date for capitalization levels is June 30, necessitating compliance in the fiscal year ending after such date. SOX compliance extends the scope of financial reporting to include the quarterly filings (but currently not the proxy information).

FDICIA VS. SOX VS. COSO – IMPORTANT DISTINCTIONS

COSO

The Committee of Sponsoring Organizations is a collaborative effort of the American Accounting Association, AICPA, Financial Executives International, The Association of Accountants and Financial Professionals in Business, and the Institute of Internal Auditors (IIA).

COSO is the source of suggested methodology for both SOX and FDICIA, and although not dictated by the FDIC, has become accepted as best practice throughout the banking industry. It is important to be clear that COSO is not a regulatory or enforcement agency.

COSO's salient document dates to 1992, with a preponderance of additional working tools over the past 20 years. In 2013, COSO rolled out an updated document that takes effect 12/15/14. COSO 2013 will need to be in effect for 12/31/14 assertions.

FDICIA 101

- Holdings at $1 billion level, necessitating FDICIA compliance by year-end
- Overall, financial reporting controls are the sole focus of FDICIA compliance
- Law requires “assertion” by CEO and CFO that control structure has integrity
- Yes! Is the answer to the question “do you have sacred, well-documented controls?”
- Starting point is a comprehensive process map of the institution
- High risk, significant financial reporting vulnerabilities need to be identified
- Internal control objectives and auditable evidence must be clearly articulated
- Testing, testing, testing

FDIC SAYS "COSO IS SUITABLE"

"In the United States, Internal Control—Integrated Framework, including its addendum on safeguarding assets, which was published by the Committee of Sponsoring Organizations of the Treadway Commission, and is known as the COSO report, provides a suitable and recognized framework for purposes of management's assessment. Other suitable frameworks have been published in other countries or may be developed in the future. Such other suitable frameworks may be used by management and the institution's independent public accountant in assessments, attestations, and audits of internal control over financial reporting."

COSO'S TIMING

Throughout this multi-year project, the COSO Board has emphasized that the key concepts and principles embedded in the original Framework remain fundamentally sound for designing, implementing, and maintaining systems of internal control and assessing their effectiveness.

Therefore, COSO will continue to make the original Framework available through December 15, 2014, at which time the 1992 Framework will be considered superseded. During this transition period—today through December 15, 2014—COSO believes continued use of the 1992 Framework is acceptable. Entities leveraging COSO's Internal Control—Integrated Framework for external reporting purposes during the transition period, however, should clearly disclose whether they used the 1992 or 2013 version.

REPORTING DEFICIENCIES - HERE'S WHAT A "BAD" EXTERNAL AUDIT LOOKS LIKE

Would we want to include this kind of language in our annual report?

- We **did not** maintain effective company-level controls
- Our control environment **did not sufficiently promote integrity and ethical values** over financial reporting
- We had **inadequate** monitoring controls, including **inadequate** staffing and procedures
- There was **inadequate** communication from management to employees regarding the importance of controls and employees' duties and control responsibilities
- We had **inadequate** procedures and controls to ensure proper segregation of duties
- We had **inadequate** policies, procedures, and personnel to ensure that accurate, reliable interim, and annual financial statements were prepared and reviewed
- We had **insufficient** levels of supporting documentation
- We had **inadequate** review procedures over account reconciliations
- Our review procedures over accounting for revenue recognition were **not functioning** effectively
- As a result of these **material weaknesses** in the Company's internal control over financial reporting, management has concluded that the Company's **internal control over financial reporting was not effective**

The company: Central Parking Corporation – 12/31/05 10-K filing with SEC – all of the above required to be included in their annual report to shareholders!

BEST PRACTICE METHODOLOGY PRE-COSO-2013

IDENTIFY PROCESSES "TOUCHING" FINANCIAL REPORTING

"CULL" OUT INSIGNIFICANT PROCESS AND ID RISKS/CONTROLS

FINANCIAL STATEMENT LINKAGE (BY OBJECTIVE NOT GL #)

EXAMPLE:

INVESTMENTS – 4 REPORTING OBJECTIVES

- TRANSACTIONS AUTHORIZED
- ACCURATE AND COMPLETE RECORDING
- SAFEKEEPING
- VALUED CORRECTLY

THE CLARITY OF ARTICULATION – CUSS

RISK AND CONTROL NARRATIVES SHOULD BE ARTICULATED CAREFULLY AND CLEARLY

AN APPLE PIE ANALOGY

C.U.S.S.

Clear – Unambiguous – Succinct - Supportable

ASK TOUGH QUESTIONS

From Billy Collins collection “Sailing Alone Around the Room”, and a poem entitled “I Chop Some Parsley While Listening to Art Blakey’s Version of Three Blind Mice”:

And I start wondering how they came to be blind

If it was congenital, they could be brothers and sisters

Or was it a common accident, all three caught perhaps in a searing explosion, fireworks perhaps?

If not, if each came to their blindness separately, how did they ever manage to find one another?

Would it not be difficult for a blind mouse to locate even one fellow mouse with vision, let alone two other blind ones?

All good questions, wouldn’t you agree?

ALL THE ELEMENTS OF RISK IDENTIFICATION IN 1 SONG TITLE

Oh My God, The Bar's on Fire, Somebody Save the Beer

By the Bottle Rockets

Risk Identification – *Oh My God, The Bar's on Fire*

Risk Articulation – *The Bar's on Fire*

Ownership – *Somebody*

Risk Remediation – *Save the Beer*

All that's missing is the control statement

Find the Risk – Articulate how it is Controlled

CLARITY AS AN AID TO TESTING SIMPLIFICATION

Mission of “tester” is not to re-audit whether the transaction is correct

Mission is to test if controls are **“sacredly” deployed**

The difference between internal audit and controls testing

AUDIT VS. TEST

KEY CONTROLS ONLY – RISK-WEIGHTED

The risk rating is easy. If our control fails, here's a handy scale to measure your CEO's reaction

L = Low-key, Laid Back

M = Mad, Miffed

H = Hot, Horrified, Hysterical

EXTERNAL AUDIT ROLE AND VIEWPOINT

- Fraud risk assessment considerations
- Auditor's role with bank implementation
- Auditor's opinion on internal control over financial reporting (ICFR)

FRAUD RISK ASSESSMENT CONSIDERATIONS

- Plan and coordinate
- What could go wrong
    - Types of Fraud
    - Factors impacting fraud risk
    - Management override of controls
- Design and implement
- Test effectiveness of controls
- Ongoing Monitoring

AUDITOR'S ROLE

- Educate – audit committees, internal audit, and management
- Implementation and external audit timeline
- Evaluate design (2nd and 3rd quarter)
- Complete interim testing (4th quarter)
- Roll forward interim testing and report on ICFR (12/31 thru fieldwork)

AUDITOR'S RESPONSIBILITY

- Test internal controls over financial reporting
- Opine on internal controls over financial reporting (integrated audit)
    - AT 501
    - 404(b) – public float over $75 million
- Report material weaknesses in ICFR

ROLLING COSO FORWARD

What has really changed?

Expansion of relative financial reporting “vehicles”?

Should we focus on internal reporting as well?

Added emphasis on risk and fraud (example on following slide)

Added emphasis on entity-level integrity via specific focus points

Do we map to the 87 focus points?

EMPHASIS ON PERFORMANCE

In the accountability objective:

- **Performance Measures Established**
- **Performance Measures Evaluated**
- **Performance Pressures Considered**
- **Performance Rewarded / Disciplined**

In the fraud potential objective:

- **Incentives / Pressures Considered**
- **Fraud Opportunities Considered**
- **Fraud "Environment" Assessed**

COSO'S 17 OBJECTIVES

Control Environment

1. The organization demonstrates a commitment to integrity and ethical values.

2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

COSO'S 17 OBJECTIVES

Risk Assessment

6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.

9. The organization identifies and assesses changes that could significantly impact the system of internal control.

COSO'S 17 OBJECTIVES

Control Activities

10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

11. The organization selects and develops general control activities over technology to support the achievement of objectives.

12. The organization deploys control activities through policies that establish what is expected and in procedures that put policies into action.

COSO'S 17 OBJECTIVES

Information and Communication

13. The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.

14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of other components of internal control.

15. The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.

COSO'S 17 OBJECTIVES

Monitoring Activities

16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

CODIFYING AND "SHORTNAMES" (FOR MAPPING)

Hand-out as reference – go to PDF

HOW THE METHODOLOGY CHANGES - 1

In prior periods, controls were typically split into three categories: entity-level, technology, and process-specific.

An updated methodology strives to “map” to 2013 COSO.

Objectives 1 through 5, and 12 through 17, equate to a portion of the prior-period entity-level controls.

Additionally, prior period COSO compliance had identified certain “global” controls such as reconciliation oversight and budget/yield analysis as part of the entity-level set. In an effort to maintain the integrity of mapping to the 2013 COSO objectives, we suggest re-assigning those as “global” process-specific controls.

HOW THE METHODOLOGY CHANGES - 2

Objective 10 equates to the process-specific controls identified and tested (this group of controls constitutes approximately 75-80% of the controls library). This is where the combined process and financial linkage approach to controls ID comes into play.

This will not significantly change (perhaps except for inclusion of additional financial reporting).

In prior efforts, FDICIA banks focused on the year-end audited statements only and the four quarterly Call reports.

SOX banks included the 10-Qs and 10-Ks (and in some cases, voluntarily, the proxy statement as well, although not required).

HOW THE METHODOLOGY CHANGES - 3

Objective 11 equates to the technology controls identified.

Typically, controls identified in this realm focus on the “on-ramps”, (i.e. anywhere someone might access the network, core, GL, investment system, fixed asset system, Fedline, etc.)

Opinion Alert:

My view is that the new risk/fraud focus points may allow us to point to independent IT audits as a control. Typically, the line in the sand for controls ID’d for COSO equates to the following question: *“How do we assert that all is well before any internal audit review and commentary?”*

HOW THE METHODOLOGY CHANGES - 4

COSO's objectives 6 through 9 represent significant updates from the 1992 guidance which only articulated 14 objectives; expanding a single "risk" objective into four, with 27 of COSO's 87 focus points devoted to risk.

In part, the banks have identified certain risk-related controls within all three of the original categories (entity-level, process, tech).

This updated methodology segregates the risk controls into a separate and distinct fourth category.

In part, certain banking industry specific controls that had been included with the entity-level set have been re-assigned to the risk set (e.g., vendor management and loan review controls).

A LOOK AT OUR COSO CONTROL NARRATIVE

Queue the Word doc as an example