THE NAVIS GROUP

COSO Implementation

An Experiential View from the Trenches

1016 Washington St., Gloucester, MA 01930
Tel. 978.495.0915
www-navis-group.com

Introduction

David B. Sidon, CPA, Managing Consultant, The Navis Group

In the past two years, our firm has been knee-deep in COSO 2013 implementation for our client banks. We have now worked collectively on these efforts with over 20 banks and, at last count, eight different external audit firms. We decided to create this whitepaper to assemble the common themes, questions, and issues into one document that might serve as a primer, a guide, and a blueprint for the practical implications, pitfalls and benefits of the COSO/FDICIA/SOX effort.

Three voices resound within this document. In addition to my own thoughts and observations, my associates Ron Petersen and Kevin Nunes have contributed to this tome. Ron's expertise is COSO 1 through 5, which focuses on integrity, corporate governance, authorities and responsibilities, succession planning, corporate response / discipline and such. Integrity, "tone from the top", whistleblower protocols and the related response thereto are his specialties. Kevin's banking operational/finance background lends itself to the practical implications of identifying and articulating the operational controls over financial reporting.

Within, we address the following:

- FDICIA / SOX / COSO
    - Defining the acronyms
    - Identifying the requirements
    - The COSO principles and focus points
    - Roles and Responsibilities for COSO implementation and management
- Sequencing the Implementation of the Principles
    - COSO Principles 10 – 12 - The Process – identifying key controls
        - Operational control considerations, observations, experiences
        - Technology's place as a foundation stone for financial reporting integrity
        - Polices and procedures
    - COSO Principles 1 – 5
        - What's required
        - What we have found
        - What we think we should be finding
        - How an institution might enhance the culture of integrity
    - COSO Principles 6 – 9
        - Identifying risk / fraud mechanisms
        - Getting from informal to formal with respect to risk
    - COSO Principles 13 – 17
        - Communications
        - Monitoring
    - Wrapping it up – Final Observations on COSO 2013 Implementation
- Appendix A - COSO's Principles & Focus Points
- Appendix B – Control Objectives – Financial Linkage Codification

FDICIA / SOX / COSO – Expanding the Acronyms

A word about FDICIA / SOX / COSO

Banks may be required to affirm the integrity of financial reporting under two distinct regulatory dictates; FDICIA and/or SOX.

COSO is the methodology (not the rule/requirement).

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. (Note: the threshold for FDICIA financial reporting compliance was $500,000 until July, 2005). The "measurement" date for asset size is December 31, necessitating compliance the following year.

SOX (the Sarbanes-Oxley Act of 2002) is a non-industry specific compliance requirement for all SEC registrants (those filing Q's and K's). 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. 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 within which June 30 falls.

COSO (The Committee of Sponsoring Organizations) is a collaborative effort of the American Accounting Association, American Institute of CPAs (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 was their 1992 guidance, with a preponderance of additional working tools over the past 20 years. In 2013, COSO rolled out an updated document that took effect on 12/15/14.

FDICIA Compliance – How COSO is "Dictated"

For banks with assets in excess of $1 billion, the FDIC Improvement Act of 1991 specifies requirements as to assessments relative to the integrity of financial reporting.

In 2009, the FDIC provided further guidance via FIL 33-2009 entitled "Annual Audit and Reporting Requirements – Final Amendments to Part 363". The amendments provide enhanced guidance for compliance with FDICIA. As amended, Part 363 requires disclosure of the internal control framework utilized as well as any identified material weaknesses. This is a self-reporting exercise signed off on by the CEO and CFO. Further, this guidance clearly links the COSO methodology as an acceptable, if not preferred, framework and best-practice.

In short, the Bank needs to comply with FDICIA and identify the methodology deployed. COSO is not only best-practice, but FDIC identifies it as "suitable" (and in "back-handed" language IDs COSO as the only choice).

FDIC's key reference to COSO follows:

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.

FDICIA may be a self-reporting exercise, but external audit needs to provide an opinion as to this exercise. Perhaps the strongest link to the need for banks to fully utilize COSO falls with the external audit firms. All bank external audit firms are requiring that COSO 2013 be in place for them to opine on the adequacy of the bank's compliant methodology. This is based on their audit requirements (also part of FIL 33-2009) as peer-reviewed under PCAOB scrutiny. Banks may not be specifically and unambiguously guided in this instance, but the external firms clearly are.

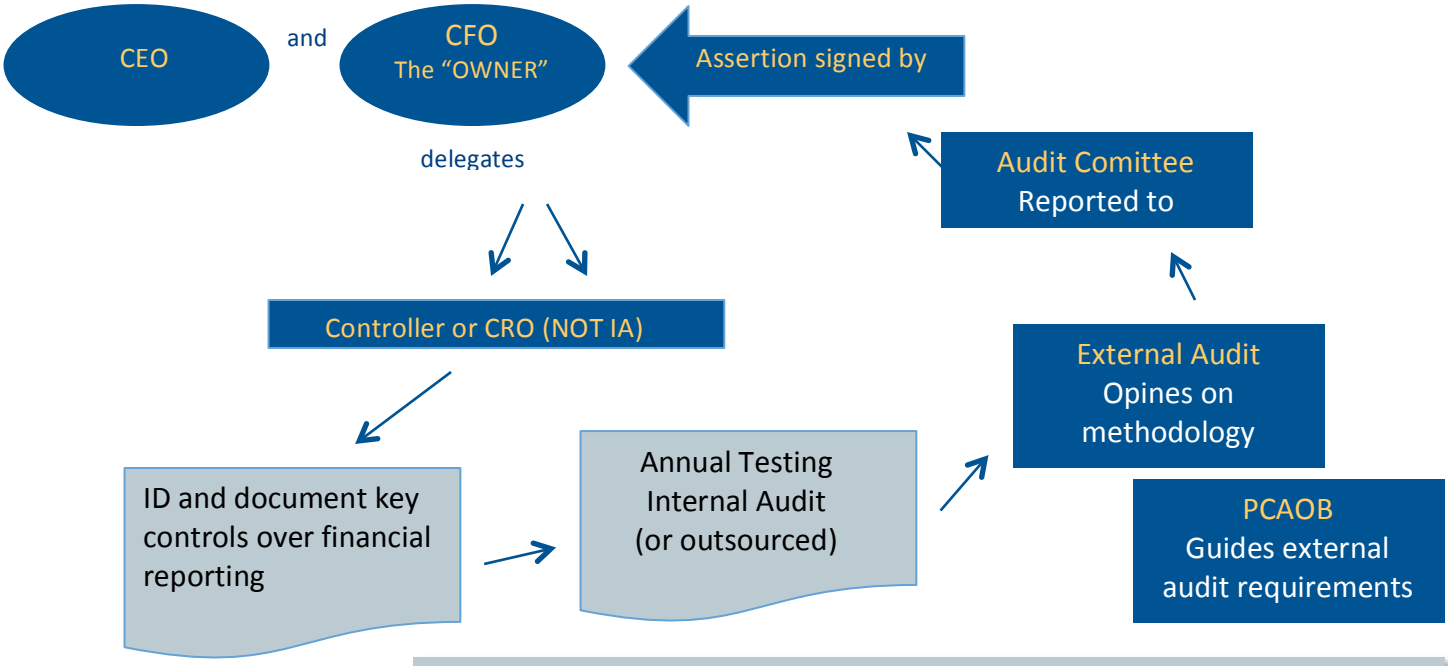
COSO's 2013 guidance includes 5 categories, 17 principles and 87 focus points with respect to financial reporting integrity. We have codified the principles and underlying focus points using a "shortname" convention for use in our methodology. The codification is included herein as Appendix A.

Roles & Responsibilities

Who owns this?

The CFO – not Internal Audit!!!

Here's the typical "best-practice" COSO operational controls organizational flow…



What's the process?
See next page

Narrating the flowchart …
The endgame is for the CEO and CFO to be able to comfortably sign an assertion letter that all is well. The CFO "owns" the effort, but typically will delegate to the Controller or CRO. Best practice has migrated away from Internal Audit's management of the task to maintain testing independence. This is the one instance that IA is "told" what to test; the CFO defines the key control universe. Testing occurs with zero tolerance; key controls are sacredly followed or not. If not, the bank would need to look for compensating controls. External audit opines on the methodology with some testing of the testing. They are guided by PCAOB standards. Keep the Audit Committee in the loop, have control owner sign-offs "roll-up", and CEO and CFO should be comfortable to sign off at year-end.

Starting with COSO Principles 10 – 12 – The Process – Identifying Key Controls

"Old School" FDICIA /SOX / COSO was focused on departmental processes. Best-practice now gives financial reporting the heavier weight, but still both process and financial reporting significance apply.

So how do we tackle this? When we go hunting for the sub-set of key financial reporting controls within the hundreds and perhaps thousands of controls institution wide, we are basically hanging the same ornaments on two different trees – process and financial aspects.

Here are the steps ….

1. Establish which processes impact financial reporting in a significant manner (this is not necessarily a departmental approach as some processes "straddle" departments)
2. Identify the key controls governing the process
3. Articulate control descriptions and auditable evidence
4. Establish financial reporting objectives (sequence = policies, tech/admin underpinnings, Balance Sheet, P&L, Footnotes)

Here's how we have approached these projects ….

Whether we are working with a newly-minted billion dollar bank undertaking FDICIA for the first time, or a bank subject to SOX, or refreshing and re-working a long established matrix, our approach is the same.

Education is job one. Typically we are providing a COSO 101 primer for management, the Audit Committee, the Board.

And then we start with principles 10, 11 and 12, which address operational controls, technology controls and policies and procedures.

As previously introduced, COSO 2013 guidance includes 5 categories and 17 principles. Category 3 – Control Activities – includes Principles 10-12, which are entirely focused on the controls that shine a bright spotlight on financial statement integrity. That's where we start. Principles 10 through 12:

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

Distilling the Control Library from 773 to 100 …

In one instance of assisting a client bank with a "refresh" of the FDICIA matrices for COSO 2013 alignment, we started with a set of 30-odd departmental matrices, that, when "stacked", produced an Excel sheet with 3,962 rows. Initial analysis determined that there were 773 controls articulated overall. Further analysis identified 177 as absolutely (as in copy-paste) redundant, 168 as insignificant with respect to financial reporting, and 253 as not at all applicable to financial reporting. One of the more interesting redundancies was that each department listed the FDICIA process as a control unto itself; one of those "loops" that the process served as a control for the process. Further refinement as the project unfolded identified additional opportunities for combinations and eliminations, such that the final distillate articulated a key financial reporting controls library numbering approximately 100.

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

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

To address the three principles above within the broader framework of a full COSO 2013 engagement, we have developed a control matrix that generally returns anywhere from 100-120 controls (+/- a few depending on the complexity of a given financial institution's business operations) covering the full spectrum of financial statement integrity. The matrix describes each control, its purpose, how it is implemented, how it is documented (more on this later), who owns/co-owns it and how it is to be tested. Because the matrix is solely focused on financial statement integrity, we avoid getting bogged down by the trap of approaching COSO 2013 compliance as if it is another backbreaking form of internal or compliance audit.

We have identified a financial reporting control structure and codified it as part of our methodology. The codification is included herein as Appendix B.

In identifying key controls, financial reporting applicability and significance offer a starting point. The controls themselves offer some interesting challenges. Are they sacred and effective, with documentary evidence left behind that may be tested or audited? One interesting example of the identification / articulation conundrum is a bank's control(s) over deposit rate index tables within the core system. Is this really a financial reporting concern? Is it significant? Who decides to change rates? How is that decision documented? How is that communicated? How does that decision reach the core system? What is the doer/ reviewer protocol? Any of that testable? Let's explore.

First, does this control belong in our matrix as a key control over financial reporting? External audit provider opinions vary on this one. If we mess up the rate change protocol for core rates, we impact thousands of accounts, so in that respect, it is a big deal. But what's the financial reporting implication? If a deposit rate is set higher than intended, customers earn more than intended, and the error will be corrected when discovered. In the meantime, what's the financial reporting implication? None! Interest expense will properly reflect the inflated pay-out. If a deposit rate is set lower than is offered / disclosed to the customer, we have a different issue. We would still be properly reflecting interest paid to customers, but we would have a lurking and growing adjustment on our hands; a sort-of financial reporting "coming attraction". Significant? Your call. That said, we always err on the side of caution and include this control in our clients' matrices.

The deposit rate decision process varies from bank to bank. Perhaps one person, the CFO or COO takes a look at market and/or competitor rates with some set frequency (weekly, monthly, quarterly, or when prodded by market, strategic or competitive shifts). Or perhaps all deposit rate decisions are ALCO driven, with the monthly meeting resulting in rate direction. Or perhaps there is a rate committee of sorts; maybe a retail or pricing committee that meets regularly. In our experience we have seen all of the above, and all three modes share the same challenge - documentation. Is an e-mail from the CFO to Deposit Operations (or wherever rates are input) sufficient to demonstrate authority to change rates? Is an e-mail emanating from the ALCO or Rate Committee meeting adequate to the task? Certainly a signed / initialed authorization of some sort would be best. And then, how does deposit ops document their process? And, one more question, if no change is warranted this period, how would deposit ops know whether they missed the e-mail / document or not?

Controls sometimes lose their way …

Here's an example of a real-life "gold standard" for this control process that fell off the rails at one of our institutions. Qwerty Bank had a very formal deposit rate protocol a few years back. A Rate Committee met faithfully every Monday. Chaired by the COO, leaders from finance, retail and deposit ops were all in the room. No minutes were kept, but a standard Excel-based rate sheet formed the basis for documentation. Bank and competitor rates were presented; strategic decisions made. Rate changes were entered onto the sheet, the COO signed off, and deposit operations walked out of the meeting with written authorization and instruction. The form was utilized even if no rate changes were made; with a "no change" check box provided. The form also provided signature/date blocks for back-office personnel performing input and QC. Perfect! So what happened? Two things. Rates weren't moving. Pretty silly to meet every Monday when rates just aren't going to change. Sort of like the loan rate change protocol documenting a prime rate that hasn't moved in many years. Organizational changes also altered the protocol. The committee stopped meeting, and when they did, two things disappeared; the sacredness of the rate change documentation, and the participation of deposit ops (they were no longer invited). The control literally died. So now what? When it comes to the COSO matrix, just what are we articulating with respect to this control?

Now let's look at investments as an example of a very straight-forward functional area. Keeping in mind that our sole goal (as it relates to investments) is to be able to specifically state that for any given financial statement investments are reported accurately, our typical matrix will identify the following investment controls:

- All investment transactions are authorized and properly documented.
- Access to investments and related records is allowed only as authorized by management.
- All securities and other investment transactions are properly recorded in detail records and accumulated, classified and summarized in control accounts.
- All securities and other investments are properly classified and valued.

To develop our investment matrix entries, we interview appropriate personnel to discuss the parameters of the investment (and/or ALM) policy, how the pre-purchase analysis is documented, how investment accounting gets done (investment accounting sub-systems, dual controls over input/verification, reconciliations to safekeeping statements, etc.), how the portfolio is priced monthly, who periodically verifies/reconciles all of this. The end result will be the identification and description of the various investment controls employed by the institution, as well as precise identification of the auditable evidence that the testers - either the bank's internal audit department, or, increasingly, an outside firm - will test. [This latter point is important since accurate identification of forms, reports, etc. makes testing much more efficient.]

The above process for investments is then repeated for all of the additional functional areas within the institution that impact information that ultimately flows to the financials – resi and commercial lending, loan ops, ALLL and problem loans, retail, e-banking, deposit ops, fixed assets/accounts payable, HR, IT, accounting/general ledger, other. The end result is a comprehensive scorecard of the institution's financial reporting testable controls, and identification of the auditable evidence (i.e., supporting documentation) that proves these controls are in place and being adhered to.

The overarching importance of documenting controls cannot be overstated; it is the "testability" of these controls that makes or breaks SOX/FDICIA compliance. There is no grading on the curve; it's pass/fail, and it only takes one failure. Many times, our interviews reveal that a given institution, like most, likely has an over-abundance of controls in place, but for some reason has decided to pass on documenting some of these controls, perhaps, for example, by not signing off on file maintenance indicating it has been properly done and reviewed with a doer/reviewer protocol, even though that is exactly how it is routinely done. As discussed below, we often can help identify where controls need to be implemented, but unquestionably where a solid control exists, it is imperative that it be properly documented.

We're often asked whether or not our 100-120 typical financial reporting controls will really pass muster when most other "brand name" solutions return more than double this amount. Although we firmly believe quality wins out over quantity every time, rather than rely on this cliché argument we point to our 20+ SOX/FDICIA clients using COSO 2013 guidance that have been tested by eight different external audit firms and reviewed by Federal and state regulators as evidence that our financial reporting controls matrix gets it right with respect to the provisions of FDICIA/SOX/COSO 2013 while being cognizant of the cost of testing the controls library.

Equating control quantities with testing dollars …

Testing samples are driven by industry standards, governed by the "frequency" of the control; annual, quarterly, monthly, weekly, daily, multiple per day.

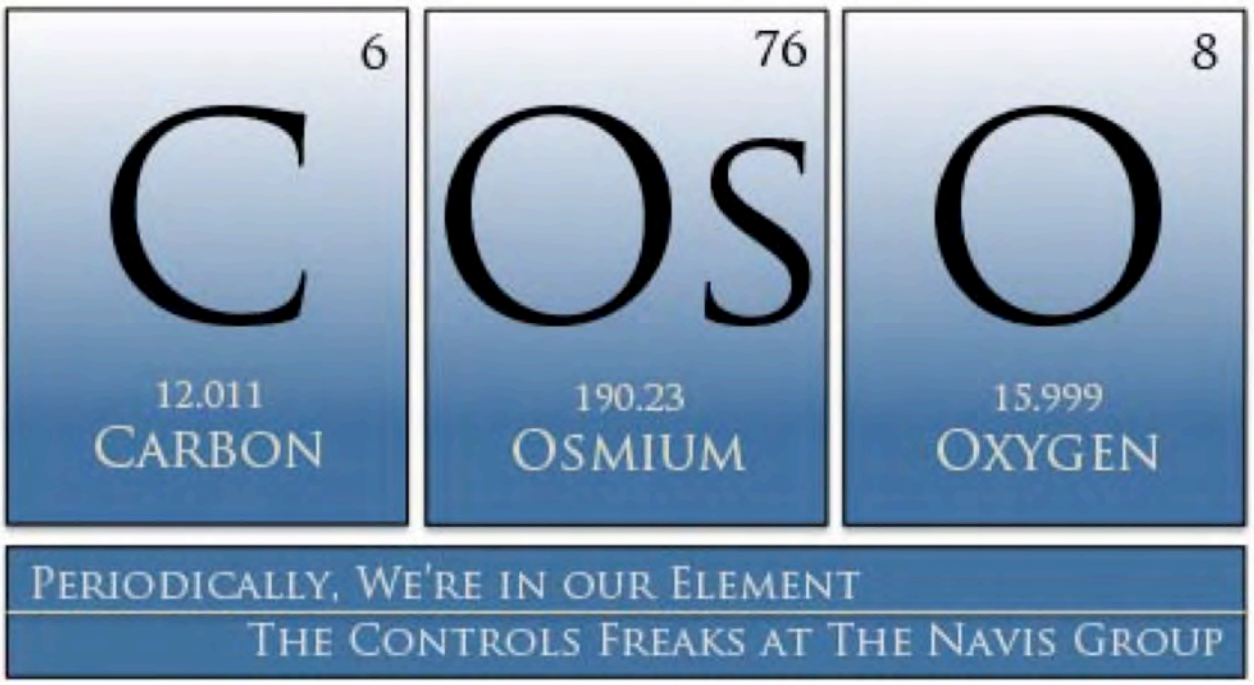
Outsourced testing engagements provide some insight into the auditing hours necessary to the effort. We have found that on average, testing requires 2 to 2 ½ hours per control per year. Assigning an hourly cost of $125 for discussion purposes, we might generalize testing costs at roughly $250 per control.

Why does this matter? Let's take a look at a couple of examples: We performed a "refresh" for a client bank that had been FDICIA compliant for years. They had identified and tested (internally) 280 controls annually. Our analysis classified 200 of the 280 as redundant, insignificant, or not applicable as financial reporting controls. We then identified 30 key controls that had been previously overlooked. The result? 170 fewer controls to test; an annual savings of over $40,000. A similar instance reduced the control count by 40, a $10,000 reduction. In both instances, the savings calculation does not include external audit savings relative to reviewing effort.

But we see a COSO engagement as even a little bit more than this. In our kick-off meetings, we emphasize that our departmental interviews will be "talk therapy" and not something to be dreaded, that our process is designed to engage in a positive dialogue those that do what they do, that we're not there to figure out what is being done wrong (we may be recovering auditors, but we're not auditors) but rather to document what is being done right, and to offer the benefit of our experiences with a wide variety of client institutions when we perceive the opportunity to add value. Inevitably, however, when we are working with a group that has not worked with us before, folks leave the kick-off meeting with that all-too-familiar "deer in the headlights" countenance.

Then a funny thing happens: post-interviews, we hear things like, "That wasn't bad" or "That was a lot easier than I expected" or "Wow, that was easy." What was anticipated to be a grueling couple of hours, with a burdensome add-on for deliverables, instead turned out to be 45 minutes to an hour whereby some of the time was, by necessity, allocated to discussing processes, policies, procedures and documentation thereof, but more time was spent exchanging ideas on best practices, and everyone left the room understanding that Navis will do the bulk of the heavy lifting. And this is exactly what it should be.

One final observation on a successful engagement: our experience across a diverse client base confirms that leadership within a given institution unequivocally determines the ultimate success and value added of our work. Someone has to be the point person for the institution; it might be the CRO, CFO or maybe the head of Internal Audit. Regardless, if that person is disengaged or is only taking ownership because he/she has to, although this won't prevent us from accomplishing our goal it will diminish the maximum value that can be obtained. Conversely, we have found that when the project owner fully embraces our work, we generally see optimization of the end result.



The Heart of the Matter - COSO Principles 1 thru 5

The Chinese symbol for INTEGRITY
"honest-behavior"

COSO is an exercise in integrity; integrity of the financial statements, and thereby the integrity of the underlying control processes. Principles 1 through 5 speak to the cultural underpinnings; "tone-from-the-top" ethical behavior, corporate governance, competencies, succession, performance pressures, measures and rewards.

When considering the COSO framework, a phrase that hits you right up front is Tone from the Top. In fact, it's the very first item. And it's not just COSO, anyone familiar with the Federal Sentencing Guidelines, Sarbanes Oxley, and numerous other legal and regulatory sources has heard the phrase before. Most seem to know that a strong Tone from the Top is essential to insuring a strong culture of integrity and compliance, but fewer know what that really means.

A strong Tone from the Top is more than the CEO and other senior leaders paying homage to integrity, and it's more than having a strong written code of conduct. Indeed, Enron had a seventy page code of conduct that was reinforced from time to time by the CEO. In fact, CEO Ken Lay backed up this code by contributing a chapter to a book entitled Ethical Leadership in Action. Unfortunately, the culture that developed in Enron allowed the value of pushing the limits of ethics and legality to overcome the values espoused in the code. The Enron CEO was convicted largely on the basis of the tone and culture that his leadership fostered rather than on direct involvement in the various frauds committed in and by the organization. The US Attorneys' Manual, which guides prosecutors in corporate prosecutions, advises that integrity and compliance programs cannot be just "paper programs", and must be "designed, implemented, reviewed, and revised, as appropriate, in an effective manner." More importantly, the Manual instructs prosecutors to determine "whether the corporation's employees are adequately informed about the compliance program and are convinced of the corporation's commitment to it."

The message to CEOs and other senior leaders is to use the bully pulpit to convey and reinforce your commitment to a strong ethical culture and your insistence that employee behavior be defined solely by integrity under all circumstances. Be sure to have a strong Code of Conduct that defines the behavior that is expected. Believe it or not, that's the easy part. Following are some additional steps that provide the building blocks of an organization that is truly imbedded with a "culture of integrity". These steps will insure that anyone who looks will know that you understand what Tone from the Top really means.

Involve the Board of Directors and senior management in the development, implementation, and operation of your ethics and compliance program.

This is more than just a good idea, and more than just meeting the COSO guidance on establishing oversight responsibility. It is also one of the seven requirements set forth by the United States Sentencing Commission (USSC) under the Federal Sentencing Guidelines in their definition of an effective compliance and ethics program. Under the heading "Organizational Leadership and a Culture of Compliance", the USSC indicates:

- The organization's governing authority shall be knowledgeable about the content and operation of the compliance and ethics program. This would normally be the CEO, the CFO, and the Board of Directors.
- The organization shall exercise reasonable oversight with respect to the implementation and effectiveness of the ethics and compliance program.
- Specific individual(s) within the highest levels of the organization shall be assigned overall responsibility for the ethics and compliance program.

As indicated above, a single individual from the senior leadership level should be designated as responsible for the program. In smaller organizations like community banks where resources may not be available for a full time assignment, the responsibility should nonetheless be assigned to a single individual as one of the "hats" he/she wears. This individual should be required to make a report to the Board of Directors (or designated Board Committee) on a regular basis. This report should include details on the status

of the ethics and compliance program and updates on any investigations that are pending that concern financial integrity or misconduct by senior officials. Executive sessions should be provided for in the Board charter. Keeping the Board involved to this degree helps meet the COSO standard that boards demonstrate independence from management and exercise oversight of the development and performance of internal control.

Establish responsibility for internal investigations within the organization

COSO recommends that organizations "address deviations in a timely manner". All organizations, small and large, should have the capability to investigate allegations, suspicious circumstances, and other indications of wrongdoing in a prompt, consistent, objective, and professional manner. While some organizations may outsource significant issues to an investigative agency or law firm, an internal capability gives the organization the ability to address smaller issues before they fester into an outsourced investigation. Smaller organizations without the resources for a full-time internal investigative function should once again assign it to a specific individual within the organization and provide that individual with appropriate policy guidance and training.

Go the extra mile on internal investigations

Don't stop with the confirmation of wrongdoing and the disposition of offenders. I suggest you dig a layer or two beneath the misconduct and take a look at the subculture and atmosphere in the unit where the misconduct occurred. Answer the question "does the tone from the top get through in this unit, or has it been translated in destructive ways?" I once managed an investigation in a bank call center that focused on collections. Management had established incentive programs to encourage employees to focus on procedures and techniques designed to increase revenues for the unit. The investigation revealed that some employees had figured out ways to manipulate performance data in a manner that fraudulently increased incentive payments to these employees, and that the practice was fairly widespread. The investigator who obtained the first employee confession during an interview asked the key follow-up question- "What made you think this was OK?" The answer was "I didn't learn right and wrong here from management; I learned it from my fellow employees". Follow-up investigation revealed that the culture in this call center was intensely numbers driven, that ethical short cuts were often encouraged with "winks and nods", and that the Tone from the Top had not come close to permeating this culture. Corrective action in this instance went well above the employees engaged in the fraudulent activity. The message here is, when you discover misconduct, peek under the covers to see what is behind it. You may not like what you find, but it's better than not finding it.

Adopt a "broken windows" approach to address ethics violations and fraud

The New York City Police Department famously brought astronomical crime rates dramatically down in part by addressing seemingly minor "quality of life" crimes. It worked. Criminologists posited that allowing minor crimes such as vandalism and subway turnstile jumping to occur without consequence creates an environment where more serious crimes will flourish. Ignoring the minor offenses sends the message that nobody cares. The same applies in business organizations. Some employees who see that minor instances as conflict of interest, data manipulation, misrepresentation, and integrity lapses going unaddressed will ask themselves "what other rules can be ignored or by-passed?" All allegations of ethical and financial rules should have a final disposition that is perceived as consistent, proportionate, and fair. This establishes valuable guardrails for your employees and makes the Tone from the Top very clear throughout the organization.

Create and maintain an atmosphere and culture where employees feel comfortable reporting violations and ethical concerns.

Don't just hire a vendor to run your ethics hotline and "check the box" on this one. In spite of improved audit techniques, enhanced technology, and better controls, studies repeatedly show that most frauds and financial misconduct are discovered as a result of someone coming forward with a tip. These studies are documented bi-annually in the Association of Certified Fraud Examiners' publication Report to the Nations.

By all means, have an ethics hotline available to your employees on a 24-7-365 basis. Sarbanes-Oxley requires organizations to have a means for employees to report violations and ethical concerns, and the USSC speaks to this issue as well. There are numerous

qualified vendors providing this service in the marketplace, and they can provide additional guidance as well. But don't leave it at that. Integrate your hotline into your culture of integrity. Make sure that your employees know senior leadership considers it important. Let them know how their anonymity (should they choose to use it) is protected, and that under no circumstances will anyone reporting concerns be retaliated against. Go beyond the hotline and create an atmosphere where employees feel comfortable reporting concerns directly to management, human resources, legal, security, or whatever channel you choose.

Turn over the rocks

If something doesn't look right, look deeper. It may be a performance metric, a quarterly report, a revenue anomaly, or anything else. Don't depend solely on your trust of a subordinate or management team. The fact is that while most employees don't commit fraud, those that do depend on your trust; they need it to conceal their nefarious acts. They depend on you to trust them and not to look too deeply. In conducting or managing hundreds of fraud investigations in business organizations, I have never seen a case where a perpetrator's managers were not shocked that an individual that they trusted could have committed such an act. This is not an appeal for cynicism, but for healthy skepticism. If you consistently require explanations, backup, and documentation for circumstances that look to be outside of your expectations, no one will be offended. Most of the time, you will find the results accurate, and if you don't, you have a head start in preventing a major problem. Perhaps Ronald Reagan was right when he defined his philosophy in dealing with nuclear disarmament talks as "trust but verify".

Beware of Willful Blindness

This is where it can get personal for senior leaders. Willful blindness, also known as conscious avoidance, is a legal doctrine that expands the definition of knowledge to the probability that a fact exists. The idea that a person can't be held legally responsible for a corrupt act or situation is no longer valid in the realm of white collar crime. The Enron and WorldCom verdicts sent a strong message that leaders should not expect to escape responsibility for the deceptive acts of others, and may be held liable even if they were not present or involved in the criminality. The US Supreme Court reaffirmed the doctrine of willful blindness in a 2011 decision. The doctrine of willful blindness adds significant importance to the recommendation to "turn over the rocks" enumerated above.

No "GEDOGEN"

We're all familiar with Amsterdam's cultural liberalism. The Dutch word is "gedogen" which translates roughly as "technically illegal, but officially over-looked".

Communicate on Ethics and Integrity with Consistency

Don't give a stirring talk on performance with integrity at one meeting, and then make a cynical comment about a legal or ethical issue at another. The second comment is likely to be transmitted through the organization as well, and is subject to being amplified and distorted along the way. This can erode your credibility, as well as your perception of your commitment to integrity. Similarly, always be conscious that the message you intend to send might not be the message that is heard. In motivating employees during "crunch" time, as in the run-up to quarter end, your statement "I don't care what it takes, we are going to meet our numbers", can easily be interpreted as a "wink and a nod" to cut corners or take ethical or even legal shortcuts.

Conclusion / Findings

In these days following the financial crisis, all financial institutions need to be mindful of restoring and maintaining public confidence in the integrity of the industry. When just one falters in this endeavor, all suffer. These suggestions are intended to assist the smaller financial organization with fewer resources to use the COSO framework and other tools in establishing a strong Culture of Integrity. The ultimate message here is don't look at COSO as just a checklist to get through, use it to insure that your organization has a genuine culture of integrity.

To date, the Navis team has guided numerous New England banks through the COSO requirement, as modified by the 2013 COSO revisions. In management's voice, we craft what turns out to be a 60 or 70 page Word document containing assertions relative to

the 17 COSO principles and their associated 87 focus points. Our goal is to produce the most positive and assertive statement, without overstating or understating the degree of the bank's adherence to the principles.

We have long held that COSO Principle 1 and its associated four focus points form the core of the COSO framework:

- The organization demonstrates a commitment to integrity and ethical values
  - Sets the Tone at the Top
  - Establishes standards of conduct
  - Evaluates adherence to standards of conduct
  - Addresses deviations in a timely manner

An organization in full, visible, and vigorous adherence to these points has what can be called a "Culture of Integrity", and will find compliance with the remaining 16 principles almost second nature. So, what have we found during the past two years of assessing COSO adherence to Principle 1? A pretty mixed bag to be sure. All of our clients were able to pass the "checklist" test, but few were able to demonstrate a living, nurtured, and ingrained "Culture of Integrity". Here are some examples in specific areas:

Codes of Conduct:
All clients have a document called a Code of Conduct, Code of Ethics, or Ethics Policy, enabling the box to be checked. Few of these documents provide a clear statement of management's expectations of behavior that complies with the law, applicable regulations, and the highest standards of integrity. Few are written in a positive, inspiring manner that can help employees navigate ethical issues that they may encounter on the job.

Whistleblower Procedures:
All clients could "check the box" here. However, most whistleblower procedures were not written or published in a way to encourage a "speak-up" culture, required for a true "Culture of Integrity". Many were hard to find and not conducive to employees wishing to express ethical concerns or questions.

Ethics/Integrity Training:
Most clients could only cite annual re-distribution and acknowledgement of the Code of Conduct as evidence of ethics training. A few had some form of mandatory on-line training. Only one demonstrated any form of live training in this area.

Internal Investigations:
Most clients provided anecdotal evidence of how deviations from integrity standards had been addressed in the past. Few could provide evidence of any process or procedure around this important area, how trends are evaluated, or how the board is informed/involved. In one case, a client reported that a customer allegation to police of fraud by the bank was being handled internally and had not been reported to the board.

Tone From the Top:
While senior leadership in most client organizations were able to point to the items that they were able to check off on the checklist, few were able to go beyond that and state how leadership reinforces its expectations of ethical behavior. One leader responded to our question on this issue by saying "I guess it's in the Ethics Policy".

Board Oversight/Involvement:
While anecdotal evidence of board involvement in specific issues was common, few had procedures and processes where regular reports were given to the board or relevant committee on the ethics/compliance program or deviations encountered.

Our overall assessment is that most of the banks that we assessed passed the COSO Principle 1 requirements with a "gentleman's C minus". This grade can be greatly improved with some effort, but with minimal additional expense. Moving toward a living, breathing Culture of Integrity benefits the brand and reputation of the institution as well as providing critical legal and regulatory protections.

Enhancing the Ethics and Compliance Program

With respect to improvement in this area, our experience with community institutions is that they do not have the resources to devote full-time personnel to all of the functions and programs that comprise an Ethics and Compliance Program. We have developed a suite of services to assist smaller organizations in accomplishing the goals of such a program within the limitations of banks where management personnel at all levels wear several hats. By undertaking some or all of the projects listed below, a smaller institution can move from "passing the COSO checklist" to a meaningful, visible, and tangible Culture of Integrity which further promotes public trust as well as important internal safeguards.

Tune up your Code of Ethics.

While the mere existence of a document entitled "Code of Ethics" does not insure a culture of integrity, it can provide a solid foundation for such a culture, as well as a useful document to help your employees navigate the integrity challenges that they face in their jobs. It should also be a powerful, positive statement of leadership's expectation of high integrity standards. Our COSO guided journey throughout New England banks has yielded good and bad news. The good news is that all of the institutions we have reviewed have a document called a Code of Ethics (or Code of Conduct, Ethics Policy, etc.) which qualifies them to "check the box" for this important COSO item. The bad news is that most of these are somewhat disjointed, arcane collections of prohibited behaviors and fall short of effectively conveying leadership's expectations and providing useful guidance to employees. An tune-up of your Code allows for transformation into a proactive and vibrant document that provides a solid foundation for your Culture of Integrity.

Tune up your "Speak-up Culture".

A strong Culture of Integrity is one where employees are comfortable and confident in reporting ethical concerns and questions. An effective whistleblower process can be an important foundation in building this comfort and confidence as it assures employees of a

"fail-safe" way to elevate a concern to high levels of leadership. As whistleblower processes are required, or at least strongly recommended in important laws and regulations, many of the institutions we have reviewed have developed a bare-bones process that is sometimes obscure in an effort to check this box. An introspective look at your entire program of encouraging employee participation in the Culture of Integrity could help remove the negative connotations that have attached themselves to the term "whistleblower".

Tune up your Ethics and Compliance Training.

Strong Cultures of Integrity, once established, require care and feeding. Effective training is one way to help insure that your culture remains healthy. Annual re-issue of the Code of Ethics and on-line training can help, but are more in the "check the box" category. The Navis Group has participated with clients in this effort, offering leadership and management training components such as "Leadership Behaviors to Promote Integrity", "Taking the Ethical Temperature of Your Unit", and "Red Flags of Ethical Misconduct", and "Fraud and Culture- the Inescapable Link".

Risk & Fraud - COSO Principles 6 thru 9

One of COSO's biggest changes in the 2013 guidance was the expansion of one risk-focused principle into four risk/fraud-focused principles. We have found it difficult to truly address the breadth of COSO's focus in crafting management assertions in the bank's "voice". Throughout the initial implementation of the entire set of COSO principles, one must remember the scoping disparity between the large Fortune 500, SEC reporting companies for whom COSO is crafted (with Sarbanes-Oxley compliance in mind) and the typical community bank striving to comply with FDICIA. Where Microsoft or Google or General Motors might have a department for each of the focus points, we can only hope that our banks have thought about the subject of each focus point and included such somewhere, sometime.

What we are finding is that we might point to existing documentation to provide the linkage to the 26 focus points under 6-9. For example, risk program documents, Risk Committee charters, Audit Committee charters and risk appetite statements demonstrate a Bank's diligence in the risk/fraud arena, thus there may be a fair bit of cut-paste in articulating management's assertions.

Consider the 26 focus points:

- Management Choices Reflected
- Risk Tolerances Articulated
- Financial Goals Incorporated
- Resource Requirements Aligned
- Accounting Standards Adhered To
- Financial Materiality Considered
- Financial Results Properly Reflected
- Reporting Standards Compliant
- External Reporting Precision Levels Appropriate
- External Reporting Appropriately Reflective
- Management Requirements Reflected
- Internal Reporting Precision Levels Appropriate
- Internal Reporting Appropriately Reflective
- Conduct Standards Compliant
- Compliance Risk Tolerance Considered
- Organizational Breadth of Risks Considered
- Internal & External Risks Considered
- Risk Mechanisms Appropriate
- Risk Significance Factored
- Risk Response Considered
- Fraud Possibilities Considered
- Incentives / Pressures Considered
- Fraud Opportunities Considered
- Fraud "Environment" Assessed
- External Changes Assessed
- Business Model Changes Assessed
- Leadership Changes Assessed

Benchmarking as a foundation for strategic opportunities relative to risk/fraud:

Rather than looking at principles 6-9 with an underlying frustration, we would suggest equating this with the newly released cyber security risk assessment tool. As we have worked with clients on the cyber assessment, two clear attributes emerge; that the tool is a terrific bench-marking exercise, and that the unfulfilled and evolving "bullets" serve as a bit of a tech strategic planning blueprint.

So too Principles 6 thru 9?

The FFIEC tool delineates "progress" along a qualitative scale of Baseline → Evolving → Intermediate → Advanced → Innovative. As viewed against the backdrop of the SEC mega-companies, our community bank score relative to Principles 6 thru 9 is probably "baseline" at best. But consider the strategic opportunity. In our discussion about Principles 1 thru 5, we emphasize the same concept; getting from baseline to an enhanced program of corporate and ethical governance. Where we might stumble trying to assert alignment with Principles 6 thru 9, we should see the opportunity presented to proactively "move the needle".

The bullet list provides us with an ERM blueprint, doesn't it? And notice the common theme as well. COSO is all about the integrity of financial reporting and the key controls underlying such. This 26 bullet list is all about environment, monitoring and reporting. To what end? In our view, undiscovered / brewing extraordinary events. These 26 bullets have no direct corollary to individual transactions or line item balances in our balance sheets, income statements and footnotes. But if a cultural breakdown leads to unnecessary risk taking, regulatory compliance gaps, behavioral lawsuits (such as harassment or wrongful termination), or compensation incentives and pressures leading the financial reporter to the dark side, then the risk/fraud controls recognize we must.

Communications & Monitoring - COSO Principles 13 thru 17

Communications and monitoring were a key element of old-COSO as well. Interestingly, as we consider the focus points articulated under these principles, our first answer might well be "Duh! We're a bank. Of course these entity-level controls are in place." This is probably a fair observation as a regulated industry. The SEC mega-companies subject to SOX may or may not have the excessive oversight that we live under in the banking industry.

One of our challenges with crafting management assertions for these principles, is that by the time we get to these final principals, we feel as though we have already addressed most of the focus points in earlier sections, especially within COSO 1 thru 5. Our assertions knowingly fell "light" for these principles, but we have become comfortable with the "pointing" technique of referencing 13-17's focus points backward to previous principles. So far, eight different external audit firms accept our approach to the last five entity-level principles.

Wrapping it up – Final Observations about COSO 2013 Implementation

Best practice has changed along the way. From 1991 when FDICIA rolled out followed by COSO in 1992, the industry's approach to this effort has matured. Sarbanes-Oxley clearly influenced the transformation. From 1991 until about 5 or 6 years ago, FDICIA compliance largely focused on departmental CRADs (as they were known in the industry) that were self-tested by each department. The testing independence question has spoken for itself and seems obvious at this post-Enron stage. The biggest evolutionary influence on COSO compliance might well be the initial SOX implementations and the subsequent studies, analysis and industry op-eds that the everyone was way out of whack with respect to the scope of the project. We earlier mentioned the banks with 773 controls and 280 controls articulated. The SOX over-scoping "eureka" moment forms the basis of the stream-lined 100 to 120 key control "right-sizing" we deploy today.

COSO 2013 brought yet another evolutionary moment, at least as it impacts our universe of FDICIA/SOX/COSO clients, and as blessed by the external firms who come in behind us to review our approach. In previous years, the entity-level control conundrum flummoxed us all. Before COSO 2013 adoption, our control matrices would typically include 14-15 so-called entity-level controls. Instead of applying management assertions to the task as we now do, and as described above, we articulated individual control descriptions with respect to COSO 1992's 14 principles and somehow finessed testing of same. Pretty silly in retrospect. Consider.

One of the long-standing principles that remain largely unchanged with COSO 2013, deals with the competency of the financial reporting group. Here's an example of a control description from a 2012 matrix: "*The company retains individuals competent in financial reporting and related oversight roles. The Finance department consists of more than 12 individuals – the principal managers include the Chief Financial Officer who is a CPA, the Comptroller who is also a CPA, and the Treasurer who has an MBA in Finance. Others in the department have varying degrees of education and years of accounting/banking experience."* This control was then tested and blessed as an accurately described and fully functioning control element. What's wrong with just asserting such? Nothing, in current best practice. The insert to the right illustrates what this looks like now within the COSO control narrative document that we deploy to map to COSO 2013's principles and focus points.

Principle 12
Focus Point 62
Personnel Competent to Execute

Performs Using Competent Personnel—Competent personnel with sufficient authority perform control activities with diligence and continuing focus.

MANAGEMENT ASSERTION:
The company retains individuals competent in financial reporting and related oversight roles. The Finance department consists of more than 12 individuals – the principal managers include the Chief Financial Officer who is a CPA, the Comptroller who is also a CPA, and the Treasurer who has an MBA in Finance. Others in the department have varying degrees of education and years of accounting/banking experience.

Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control over financial reporting. Job descriptions are maintained for all Accounting & Finance personnel.

Note: and then we insert a table with names, titles, certifications, educational attainment, and years of industry experience.

What does a complete set of fully compliant process documentation look like? External audit needs to review and re-test a Bank's COSO efforts and internal testing each year. We strive to have the following available for them:

- The Excel Workbook

Our workbook includes a number of tabs, including a "guide" that describes the approach as follows:

> COSO suggests a dual approach toward controls identification - significant processes impacting financial reporting and the financial reporting "flow" itself.
>
> 1. VETTING PROCESSES / FDICIA PROCESSES ONLY
>
> > *Herein, we take a standard list of banking processes sorted departmentally, and identify those processes that significantly impact financial reporting. The "cull" also includes taking out "control" processes - for example, reconciliations are not a banking effort, rather they act as a key control for the banking effort, and thus will be identified as controls for relevant processes. The "cull" also includes considerable judgmental combinations to ease the implementation of this methodology - example, origination, closing and funding are separate processes for every loan type - we have in all cases combined product offerings (except keeping resi and commercial processes distinct), and in may cases combined origination, closing and funding as one process.*

2. CONTROLS LINKED TO PROCESSES

Herein, we utilize the list of vetted processes as our table of contents for assigning controls applicability. This tab also is utilized to assess the fraud risk inherent in a given process, along with the bank's risk rating. This tab includes the following components:

- *Function / Process*
- *Process Fraud Potential*
- *Process Fraud Risk Assessment*
- *Control Name*

In that certain controls apply to multiple processes, color coding provides an indication of controls that are either unique to one process or not.

3. FINANCIAL REPORTING CONTROLS

For mapping controls to the financial "flow" (the more important component of this exercise), the controls library presented in the FINANCIAL REPORTING CONTROLS tab is key. Starting with policies and tech controls, then moving on to GL admin and reporting controls that "touch" all of the financial reporting, the "flow" moves in balance sheet - income statement - footnote order. In each area, overall control objectives and risk concerns are identified and the codification of the overall methodology flows as AREA-OBJECTIVE-RISK-CONTROL. For example - area C's second objective, and third control would codify as C's AREANAME-2-3.

4. CONTROLS DETAIL - EDIT - MERGE

This tab is the library of unique controls (i.e. certain controls govern multiple processes and/or financial considerations) - here they are non-redundant. The column headers for this tab include:

- *Test Group*
- *Control Group*
- *Control Name*
- *Control Objective*
- *Control Description*
- *Auditable Evidence*
- *Owner*
- *Co/owner*
- *Frequency*
- *Annual Sample Size*
- *Discussion Notes*

This tab serves as the "workspace" for developing and editing control descriptions, as well as serving as the basis of the review, sign-off and test script doc merges.

5. SAMPLE SIZE

The SAMPLE SIZE tab serves as drop down box data for the process tab.

❖ Review and Sign-off Word documents:

The Excel workbook details provide a means to perform a “docmerge” to produce individual review sheets for the control owners for editing purposes. Once edits are complete, another round of documentation gathers control owner signatures as “roll-up” of control accountability and responsibility. If we have 100 controls, we should have 100 sign-offs.

- Test Scripts:

  The Excel workbook details also provide a means to perform a "docmerge" to produce test scripts for internal or outsource resources to deploy. For our banks that outsource the testing, this is a requirement of ours (for consistency sake). For in-house IA testing, the scripts are available, but we find that sometimes IA wants to stick with their regular audit protocols.

- The COSO 2013 Narrative:

  This is the cornerstone of COSO compliance. We craft a Word document (in the "voice" of the bank) that often runs 60 or 70 pages. The document describes the institution's COSO process and maps management's assertions with respect to the principles and focus points.

How may we assist your institution with FDICIA / SOX / COSO ?

Please reach out for a "show-and-tell" and/or for a "COSO 101" session for your management team, Board of Directors and/or Audit Committee.

Visit us at www.navis-group.com - (978) 495-0915

David B. Sidon, CPA
Sidon@navis-group.com

THE NAVIS GROUP

Ronald C. Petersen
Petersen@navis-group.com

Kevin W. Nunes
Nunes@navis-group.com

Appendix A - COSO's Principles & Focus Points

COSO's 2013 guidance includes 5 categories, 17 principles and 87 focus points with respect to financial reporting integrity. We have codified the principles and underlying focus points using a "shortname" convention as follows:

Codification	COSO 2013 Principle	COSO 2013 Focus Point
1.01	Integrity	Tone at the Top Demonstrated
1.02		Ethical Standards Defined
1.03		Ethical Performance Evaluated
1.04		Conduct Deviations Addressed
2.05	Board Independent Oversight	Board Responsibilities Identified & Accepted
2.06		Board Expertise Evaluated
2.07		Board Independent
2.08		Board Oversight of Internal Control Clear
3.09	Authorities	Structure Supports Objectives
3.10		Reporting Authorities Clear
3.11		Authorities Assigned; Segregation Assured
4.12	Competency	Policies and Practices Established
4.12		Personnel & Provider Competency Evaluated
4.14		Competent Personnel Developed / Retained
4.15		Succession Planned
5.16	Accountability	Authorities & Responsibilities Enforced
5.17		Performance Measures Established
5.18		Performance Measures Evaluated
5.19		Performance Pressures Considered
5.20		Performance Rewarded / Disciplined
6.21	Risk Identification & Assessment	Management Choices Reflected
6.22		Risk Tolerances Articulated
6.23		Financial Goals Incorporated
6.24		Resource Requirements Aligned
6.25		Accounting Standards Adhered To
6.26		Financial Materiality Considered
6.27		Financial Results Properly Reflected
6.28		Reporting Standards Compliant
6.29		Reporting Precision Levels Appropriate
6.30		External Reporting Appropriately Reflective
6.31		Management Requirements Reflected
6.32		Reporting Precision Levels Appropriate
6.33		Internal Reporting Appropriately Reflective
6.34		Conduct Standards Compliant
6.35		Compliance Risk Tolerance Considered
7.36	Risk Alignment / Management	Organizational Breadth of Risks Considered
7.37		Internal & External Risks Considered
7.38		Risk Mechanisms Appropriate
7.39		Risk Significance Factored
7.40		Risk Response Considered

8.41	Fraud Potential	Fraud Possibilities Considered
8.42		Incentives / Pressures Considered
8.43		Fraud Opportunities Considered
8.44		Fraud "Environment" Assessed
9.45	Risk Profile Changes	External Changes Assessed
9.46		Business Model Changes Assessed
9.47		Leadership Changes Assessed
10.48	Control Activities	Risk Assessments Integrated
10.49		Internal & External Factors Considered
10.50		Business Process Significance Determined
10.51		Balance/Mix of Controls Considered
10.52		Activity Levels Considered
10.53		Segregation of Duties Addressed
11.54	Technology	Tech Dependency Determined
11.55		Tech Processing Reliable
11.56		Tech Access Controlled
11.57		Tech Acquisitions / Maintenance Controlled
12.58	Policies & Procedures	Policies & Procedures Extant
12.59		Policies & Procedures Executed
12.60		Control Activities Timely
12.61		Control Activities Evaluated / Corrected
12.62		Personnel Competent to Execute
12.63		Control Activities Periodically Reassessed
13.64	Relevant Information	Info Requirements Identified
13.65		Info Captured
13.66		Info Meaningfully Processed
13.67		Info Current, Accurate, Reliable
13.68		Info Levels Appropriate
14.69	Internal Communications	Internal Controls Internally Communicated
14.70		Management-Board Communications Sufficient
14.71		Separate Communications Extant
14.72		Communications Relevant
15.73	External Communications	External Parties Informed
15.74		Inbound Communications Enabled
15.75		Board Receives Important External Info
15.76		Separate Communications Extant
15.77		Communications Relevant
16.78	Monitoring - Separate Evaluations	Evaluation Mix Balanced
16.79		Business / Process Changes Considered
16.80		Baseline Understanding Established
16.81		Evaluators Knowledgeable
16.82		Evaluations and Processes Aligned
16.83		Evaluations Properly Risk-Scoped
16.84		Evaluation Feedback Enabled
17.85	Internal Control Deficiencies	Results Assessed
17.86		Deficiencies Appropriately Communicated
17.87		Corrective Actions Tracked

Appendix B – Control Objectives – Financial Linkage Codification

Financial Statement Linkage	CODIFICATION	Financial Reporting Objectives
Policies	POLICIES 1	Key policies and procedures governing financial reporting are properly articulated and communicated
Technology	TECH 1	Technology policies and user expectations are properly articulated and communicated
	TECH 2	Personnel and vendor system access is adequately controlled and monitored
General Ledger Admin & Maintenance	ADMIN 1	Access to Financial Accounting and Chart of Accounts Maintenance is properly authorized, documented and performed with appropriate segregation of duties
General Ledger - Entries and Reconciliations	GL 1	Postings to the General Ledger are complete and accurate as to account amount and period
Financial Reporting	REPORTING 1	Reporting is accurate and in conformance with GAAP, RAAP Requirements
	REPORTING 2	Monthly financial oversight is performed and documented
Cash and Equivalents	CASH 1	Access to cash and related files and records is allowed only as authorized by management.
	CASH 2	Cash Transactions/Transfers/Borrowings are accurately analyzed/calculated/executed - recorded timely and accurately
Investments	INV 1	All Investment transactions are authorized and properly documented.
	INV 2	Access to investments and related records is allowed only as authorized by management.
	INV 3	All security and other investment transactions are properly recorded in detail records and accumulated, classified and summarized in control accounts
	INV 4	All securities and other investments are properly classified and valued.
Loans	LOANS 1	All loans are appropriately approved for acceptance of credit risk.
	LOANS 2	All loans are closed and set-up in a timely and accurate manner.
	LOANS 3	Loan disbursements are recorded timely and accurately as to account, amount and period.
	LOANS 4	Loans are maintained properly; review controls effective
	LOANS 5	Loans are reported accurately with respect to FAS requirements such as FAS 91, impairment and TDR rules
	LOANS 6	Loan rate index changes are accurately processed
	LOANS 7	Additions to the allowance for loan losses and charge-offs are appropriately approved and recognized on a timely basis – Problem or Impaired loans are properly categorized, tracked and managed.
	LOANS 8	Sold and/or Participation Loans are properly reflected - gains and losses are accurately calculated
Foreclosed Assets and Other Real Estate Investments	OREO 1	All acquisitions and sales of foreclosed assets and real estate investments are authorized and properly documented.
	OREO 2	All transactions relating to foreclosed assets and real estate investments are properly recorded in detail records and accumulated, classified and summarized in

		control accounts on a timely basis
	OREO 3	All foreclosed assets and real estate investments are properly valued.
Fixed Assets	FIXED ASSETS 1	Premises and equipment are acquired only with proper authorization.
	FIXED ASSETS 2	Acquisitions and disposals of premises and equipment are properly recorded on a timely basis.
	FIXED ASSETS 3	Depreciation of premises and equipment is calculated using proper lives and amounts.
Other Assets	OTHER ASSETS 1	Accrued interest receivable is calculated correctly and recorded properly.
	OTHER ASSETS 2	Intangible and other assets are properly authorized and reflect accurate carrying values
	OTHER ASSETS 3	Amortization of assets is calculated and recorded appropriately when necessary using proper lives and amounts.
Deposit Accounts	DEPOSITS 1	All deposit account transactions are appropriately authorized.
	DEPOSITS 2	All deposit account transactions are recorded timely and accurately as to account, amount and period.
	DEPOSITS 3	Deposit accounts are maintained properly; review controls effective
	DEPOSITS 4	All deposit account transactions are properly applied to customer and general ledger accounts.
	DEPOSITS 5	All deposit account interest rates are appropriately authorized and correctly reflected in rate/index tables
Accounts Payable	A/P 1	Purchases are based on valid authorizations
	A/P 2	Expense coding is appropriate
	A/P 3	All disbursements are authorized and accurately posted to the accounting records.
Other liabilities	OTHER LIAB 1	Pension liabilities (including SERP, Defined benefit, post-retirement plan) accurately stated and changes properly reflected in P&L and AOCI
	OTHER LIAB 2	Other liabilities are properly recorded and classified in the accounts.
Equity and Regulatory Capital	EQUITY 1	All equity and Accumulated Other Comprehensive Income (AOCI) transactions are properly authorized, approved and in compliance with applicable legal and regulatory requirements.
	EQUITY 2	All equity and AOCI transactions are properly recorded on a timely basis and properly classified in the accounts.
Interest Income & Expense	INT INC/EXP 1	Interest income on loans is accurate and complete.
	INT INC/EXP 2	Interest expense on deposit products is accurate and complete.
Non-Interest Income	NON-INT INC 1	Non-interest income recognition is accurate, timely and complete.
Human Resources / Payroll	HR 1	All wages are properly authorized and approved.
	HR 2	All wage computations are accurate and properly recorded and classified in the accounts.
	HR 3	Ethical conduct expectations extant; performance reviews performed
Income Taxes	INC TAX 1	Income taxes and deferred tax assets and liabilities are properly calculated and recorded in the accounts on a timely basis.