The Navis Group
COSO / FDICIA
SOX Playbook

V 2023.3

THE NAVIS GROUP

TABLE OF CONTENTS

VERSION 2023.3 – SEPTEMBER, 2023

1. Foreword - Introduction
2. FDICIA / SOX / COSO / ICFR – Expanding the Acronyms
   - 2.5 FDICIA requirements at $500 million – A Checklist
   - 2.6 FDICIA requirements at $1 billion – A Checklist
3. COSO's Seventeen Principles
4. FDICIA Compliance – How COSO is "Dictated"
5. COSO Compliance – PCAOB as the Main Driver of Best Practice
6. COSO Compliance – Who Owns This?
7. Education – Management, Audit Committee, Board
8. Two Types of Controls – Operational vs. Entity-Level
9. Navis' Standard Control Hierarchy
10. Methodology Phase 1 – Pre-Planning (profile, policies/procedures, group sessions)
11. Methodology Phase 2 – Kick-off Meeting – All Hands
12. Methodology Phase 3 – Functional Walk-Through Sessions
    - 12.V Virtual Walk-Through Sessions
13. Methodology Phase 4 – Documentation – Request, Accumulation, Secure Portal
14. Methodology Phase 5 – Navis' Initial Draft of Control Descriptions, Attributes
15. Methodology Phase 6 – Control Owners & Task Performers
16. Methodology Phase 7 – Control Owner(s) Review, Assimilation, Sign-off
17. Controls Considerations – Applicability
18. Controls Considerations – Significance Standards
19. Controls Considerations – Control Design
    - 19.5 Controls Considerations – Management Review Controls - Precision
20. Controls Considerations – Auditable Evidence
21. Introduction to the COSO Narrative – Qualitative Assertions
22. COSO Narrative Interviews
23. FDICIA / SOX / COSO Project Timeline
24. Testing – Test Scripts; Timing; Feedback Loop
    - 24.5 Testing Independence
25. Testing – Annual Sample Sizes
26. Smartsheets for Update and Annual/Quarterly Controls Certifications

1 FOREWORD - INTRODUCTION

Over the past dozen or so years, The Navis Group has had the privilege of working with more than 50 financial institutions on COSO / FDICIA / SOX compliance. We've learned and grown over the years as best practice has evolved, and especially as the COSO 2013 update has taken hold. We've been guided by some terrific audit firms and audit partners and managers, who in turn have been guided by the FDIC and PCAOB.

We've created, and tweaked, and re-worked our approach and methodology, a seemingly never-ending continuum and feedback loop. As we've delivered sales demos, educational meetings, and kick-off sessions, we've a developed our own "style" as well as a standard description of our approach to COSO that begged to be put down on paper as a bit of a COSO / FDICIA / SOX manual; our playbook.

We've written this with multiple constituencies of readers in mind. First and foremost, we wanted folks approaching this project for the first time to understand the totality of the effort, while providing some comfort that this is less daunting than it may seem. Boards and Audit Committees should benefit from this, as well as external audit firms or partners encountering our approach for the first time.

Your suggestions are welcome. Hope this helps.

Best,
Dave Sidon
Kevin Nunes
The Navis Group

2 COSO / FDICIA / SOX – EXPANDING THE ACRONYMS

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 full FDICIA financial reporting compliance was $500,000 until July, 2005). The $500 million threshold still carries a number oif requirements – see Topic 2.5. The "measurement" date for asset size is fiscal year-end (typically 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). SEC registrants designated as "emerging growth companies" are granted an additional length of time for compliance, albeit, most banks may strategically wish to declare SOX compliance, instead of citing to shareholders that it's OK to defer. 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. The AICPA offers a "COSO Internal Control Certification Program".

2.5 FDICIA REQUIREMENTS AT $500 MILLION – A CHECKLIST

In the year that a bank's assets exceed $500 million as midnight dawns on a year (within seconds of the New year's ball drop in Times Square), here are the things (in checklist format) that need to be in place …..

- ☐ We have a separate Audit Committee whose responsibilities are clear (best if charter exists)
- ☐ All of our Audit Committee members are outside directors and a majority of those members are independent from management

Audited financial statements:

- ☐ Audited financial statements submitted to our primary regulator within 120 days
- ☐ Our auditor is independent in the eyes of the AICPA, SEC, PCAOB (as applicable)
- ☐ Our audit firm no longer performs any non-attest functions for us
- ☐ Our audit firm assures partner rotation on a five-year cycle

Along with the audited financial statements, we are submitting a statement asserting these 3 elements:

- ☐ Management is responsible for and has prepared the financial statements prior to audit review
- ☐ Management has established & maintains an adequate control structure over financial reports
- ☐ Management (and thereby, the bank) complies with all safety & soundness laws & regulations

15 days after receipt of the audited statements, we need to file these 2 items with our regulator

- ☐ The audit firm's governance communication (responsibilities, etc)
- ☐ The audit firm's control weakness / deficiency findings / report (if applicable)

2.6 FDICIA REQUIREMENTS AT $1 BILLION – A CHECKLIST

In the year that a bank's assets exceed $1 billion as midnight dawns on a year (within seconds of the New year's ball drop in Times Square), here are the things (in checklist format) that need to be in place in addition to everything we have been doing since we hit $500 million …

- ☐ Our Audit Committee is completely composed of outside directors, independent from management

In addition to the three items required in management's statement at $500 million, 3 more now apply:

- ☐ A statement identifying the control framework that we have deployed
- ☐ A statement that the assessment included our call Report filings
- ☐ Our assessment as to the adequacy of the control structure

For the current year, we have:

- ☐ Reviewed and updated our control structure
- ☐ Tested key controls over financial reporting
- ☐ We mitigated any control gaps
- ☐ Had control owners sign off (accountability)
- ☐ Assured proper linkage with the COSO guidance
- ☐ Assured proper linkage with our financial statements

3 COSO'S SEVENTEEN PRINCIPLES

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.

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.

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.

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.

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.

4 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.

5 COSO COMPLIANCE – PCAOB AS THE MAIN DRIVER OF BEST PRACTICE

If COSO guidance is esoteric and philosophical offering meager doses of practical direction, and the FDICIA requirements merely point to COSO as our beacon, where's the playbook? That question is, in part, why we have crafted this document.

In sitting through the AICPA's COSO Certification Program, the participants are reminded continually that COSO is non-prescriptive. This is obvious in one regard, since COSO is designed with all SEC-reporting entities in mind, thereby applying to Apple, Google, General Motors, and McDonald's, as well as the local bank hitting the $1 billion threshold. Examples regarding inventories, income recognition, and R&D expenditures are not useful for our industry. Control examples regarding loan impairment, TDRs, OTTI, loan risk ratings, wire processing and ACH processing are non-extant.

Our real source of guidance is our external financial statement audit firms, via review as we implement our controls identification and documentation, and through audit commentary at year-end. The hidden driver (for banks) is the PCAOB. As the PCAOB audits our auditors, their "hot buttons" become evident. It's frustrating for most bankers that there is not a straight-line connecting PCAOB's focus and an individual bank's COSO compliance. As a provider of COSO implementation and management services, we similarly struggle, but have the benefit of hearing from multiple external audit firms each and every year, with some sub-set thereof undoubtedly recently reviewed by PCAOB.

The PCAOB does issue "Staff Audit Practice Alerts" which are available to all at www.pcaobus.org. The PCAOB self-describes these alerts as follows: "Staff Audit Practice Alerts highlight new, emerging, or otherwise noteworthy circumstances that may affect how auditors conduct audits under the existing requirements of the standards and rules of the PCAOB and relevant laws."

Alert Number 11, issued on October 24, 2013 is an important document for COSO compliance. Entitled "Considerations for Audits of Internal Control over Financial Reporting", it covers:

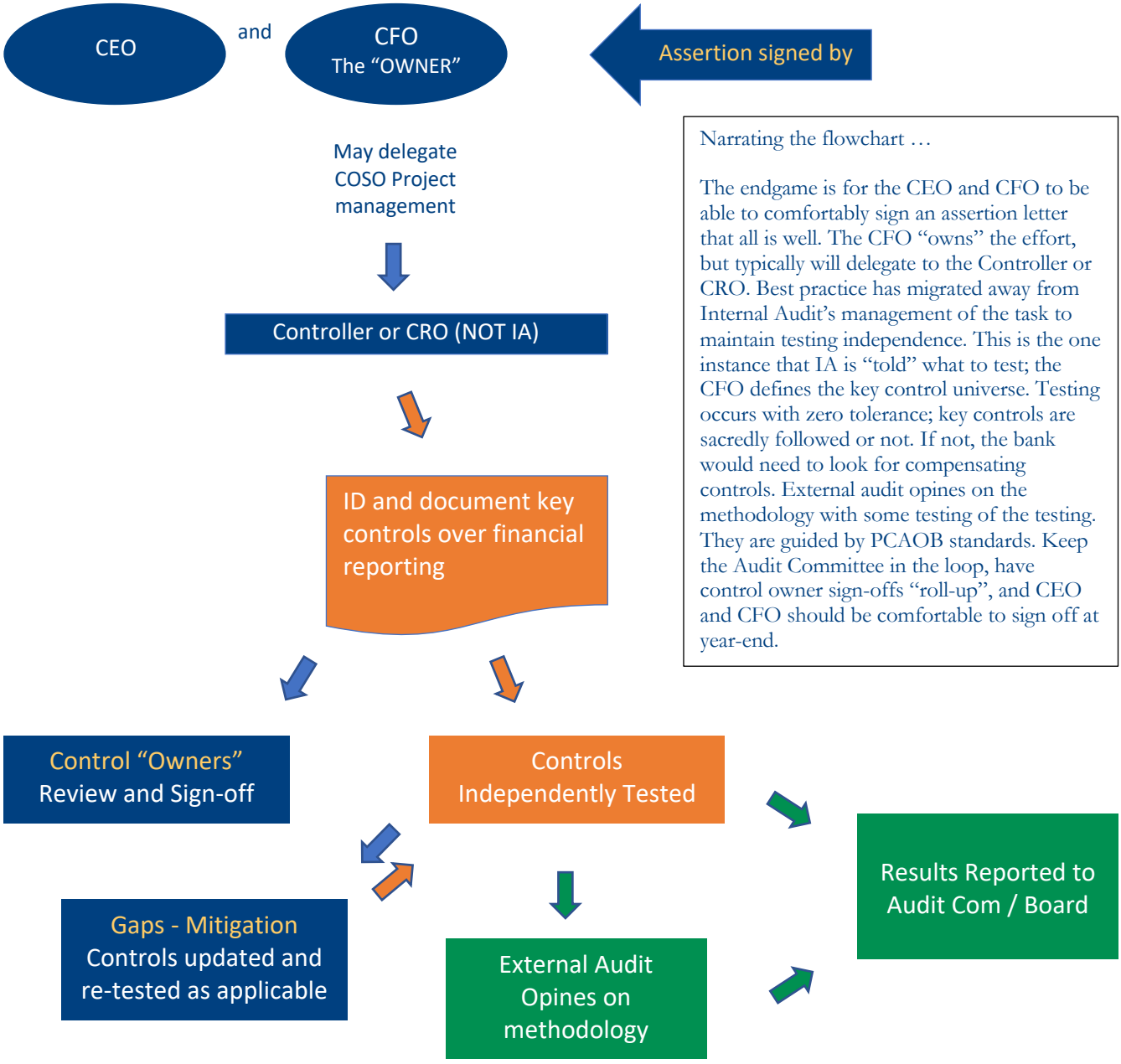
- Risk assessment and the audit of internal control
- Selecting controls to test
- Testing management review controls
- Information technology ("IT") considerations, including system- generated data and reports
- Roll-forward of controls tested at an interim date
- Using the work of others
- Evaluating identified control deficiencies

6 COSO COMPLIANCE – WHO "OWNS" THIS?

Who owns this?

The CFO – not Internal Audit!!!

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



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.

7 EDUCATION – MANAGEMENT, AUDIT COMMITTEE, BOARD

Good COSO practice starts with educating all the stakeholders, including the full spectrum of people from control operational owners to the Board. Our business model includes a sales demo that really doubles as a COSO 101 class. Often we are invited to speak to the Audit Committee and/or Board either pre-project or early in the process to provide this education. Our Powerpoint deck is periodically updated and is posted on our website and available to all (www.navis-group.com).

When we start an implementation project, we have always commenced with an hour-long kick-off meeting to talk about the requirements and the process, and to set everyone's mind at ease that this won't be such a daunting project. In the kick-off, we are especially looking for the CEO or CFO to set the tone for project, letting everyone know just how important this financial reporting integrity exercise is.

In recent years, we've encountered client banks that make a habit of "learning lunches", a concept we've come to embrace. Well in advance of a project kick-off, meeting with management and the operational folks who are truly the control owners has tremendous merit.

As a provider of COSO compliance assistance, we also regularly meet with the external audit firms that will be opining on the methodology. These professionals are not in need of COSO education, but rather benefit from us providing a "cook's tour" of the how's and why's and scope of our approach.

8 TWO TYPES OF CONTROLS – OPERATIONAL VS. ENTITY-LEVEL

In the AICPA's COSO Certification Program, there is a continual reminder that COSO guidance is "non-prescriptive". Simply enough, it is a reminder that circumstances, processes, significance, and thereby, judgement, dictate our implementations for FDICIA and SOX. That COSO is not industry specific is exasperating enough, but the lack of regulatory guidance on this requirement leads to considerable, unnecessary interpretation and differences of opinion.

The philosophy of operational versus entity-level controls requires such interpretation. Principle 1, Focus Point 1 helps frame this challenge: "Integrity / Tone at the Top". Every bank has an Ethics Policy or Code of Conduct. That the Board reviews and approves the policy each year is an auditable event memorialized in Board minutes. That employees read and acknowledge the document at hire and at an annual anniversary is an auditable event. Pass/ fail grades may be assigned. That a culture of integrity permeates the enterprise is another matter entirely. How is that tested, proven, graded? Anecdotally, and in our methodology, via management assertions in our narrative document (see pages addressing the narrative for specifics). That the CEO contributes to employee on-boarding with a "chat" that includes the integrity message; that a cultural values statement speaks to integrity; that the performance reviews include an integrity factor, and that cultural components of training and whistle-blower protocols set a tone, are indications relative to integrity, albeit un-auditable.

Thus, the two prongs of our COSO / FDICIA / SOX methodology.

Operational Controls

In our experience a typical institution will identify between 90 and 125 key controls over financial reporting. Many mature compliers that may have undertaken the COSO process ten or more years ago may find themselves with hundreds more (good time for a "refresh" to save some annual testing dollars). We are comfortable with 90-125 range based on multiple projects, and multiple audit firms helping to form this consensus.

Entity-Level Controls

Our narrative containing management assertions relative to entity-level, qualitative, cultural, and organizational controls has also been vetted and accepted by multiple audit firms. Above, we listed integrity as an example. Other examples of controls best covered is the assertive narrative mode include:

- Corporate Governance
- Audit Committee Charter (Roles)
- Org Chart (Clarity & Communication)
- Succession Planning
- Risk Management
- Fraud Management
- Technology Infrastructure
- Info Security (Social Engineering)
- Compliance
- Audit - Three Lines of Defense

9 NAVIS' STANDARD CONTROL HIERARCHY

For this section, we need to break from our one-pager approach in order to fit the complete structure.

For banks, we have created the following controls structure. This is the "tree" on which we hang our control "ornaments".

A word about "mapping".

Legacy COSO projects have struggled with the issue of mapping the control structure back to COSO's 17 principles and 87 focus points, as well as mapping back to the financial statements, which is what this is all about in the end.

Our methodology solves the mapping conundrum and that crazy 87 column spreadsheet by utilizing a table of contents that "embeds" the COSO and financial statement linkage. By delineating the COSO principles as the primary table of contents "flow" and financial statement order as the secondary table of contents category, linkage is established and clear.

Princ.	COSO – Financial Statement Linkage	Codification	Financial Reporting Objectives
1	Integrity Ethical Standards	ETH 1	Ethical conduct expectations extant, inclusive of personnel and/or director acknowledgements thereof.
5	Accountability Performance Standards	PERF 1	Performance reviews performed and documented.
10	Control Activities		
	General Ledger	GL 0	Access to financial accounting systems is properly authorized, documented and performed with appropriate segregation of duties. Periodic monitoring of system access is performed and, as applicable, SOC reports are reviewed for control considerations.
		GL 1	Access to Chart of Accounts Maintenance is properly authorized, documented and performed with appropriate segregation of duties.
		GL 2	Postings to the General Ledger and reconciliations are complete, timely and accurate as to account amount and period.
	Financial Reporting	REP 1	Monthly financial oversight is performed and documented.
		REP 2	Call Report is accurate and in conformance with GAAP, RAAP Requirements.
		REP 3	Year-end audited financial statements and associated footnotes are accurate and in conformance with GAAP, RAAP Requirements.
		REP 4	SEC reporting is accurate, complete and timely (if applicable – stock banks only for SOX compliance.
		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.
		INV 0	Access to systems utilized for investment accounting is properly authorized, documented and performed with appropriate segregation of

Princ.	COSO – Financial Statement Linkage	Codification	Financial Reporting Objectives
			duties. Periodic monitoring of system access is performed and, as applicable, SOC reports are reviewed for control considerations.
	Investments	INV 1	All Investment transactions are authorized and properly documented.
		INV 2	All security and other investment transactions are properly recorded in detail records and accumulated, classified and summarized in control accounts.
		INV 3	Access to investments and related records is allowed only as authorized by management.
		INV 4	All securities and other investments are properly classified and valued.
	Residential and Consumer Lending & Servicing	RESI 0	Access to systems utilized for residential loan origination, approval and on-boarding is properly authorized, documented and performed with appropriate segregation of duties. Periodic monitoring of system access is performed and, as applicable, SOC reports are reviewed for control considerations.
		RESI 1	All loans are appropriately approved for acceptance of credit risk.
		RESI 2	All loans are closed and set-up in a timely and accurate manner.
		RESI 3	Loan disbursements are recorded timely and accurately as to account, amount and period.
		RESI 4	Loans are maintained properly; review controls effective.
		RESI 5	Loans are reported accurately with respect to FAS requirements.
		RESI 6	Loan rate index changes are accurately processed.
	Commercial Lending & Servicing	COMM 0	Access to systems utilized for commercial loan origination, approval and on-boarding is properly authorized, documented and performed with appropriate segregation of duties. Periodic monitoring of system access is performed and, as applicable, SOC reports are reviewed for control considerations.
		COMM 1	All loans are appropriately approved for acceptance of credit risk.
		COMM 2	All loans are closed and set-up in a timely and accurate manner.
		COMM 3	Loan disbursements are recorded timely and accurately as to account, amount and period.
		COMM 4	Loans are maintained properly; review controls effective.
		COMM 5	Loan rate index changes are accurately processed.
	Allowance for Credit Losses on Loans	ACLL 0	Access to systems utilized for allowance calculations is properly authorized, documented and performed with appropriate segregation of duties. Periodic monitoring of system access is performed and, as applicable, SOC reports are reviewed for control considerations.
		ACLL 1	Problem or Impaired loans are properly risk rated; TDR determinations for modifications documented; impairment and write-down calculations documented.
		ACLL 2	Credit quality review extant; Problem or Impaired loans are properly tracked.
		ACLL 3	Additions to ACLL and charge-offs are appropriately calculated, justified, approved and timely; FAS requirements met.
	Sold, Participation, Other Loans	OTH LOANS 1	Sold and/or Participation Loans are properly reflected - gains and losses are accurately calculated.
	Fixed Assets	FIX 1	Premises and equipment are acquired only with proper authorization.
		FIX 2	Acquisitions and disposals of premises and equipment are properly recorded on a timely basis.

Princ.	COSO – Financial Statement Linkage	Codification	Financial Reporting Objectives
		FIX 3	Depreciation of premises and equipment is calculated using proper lives and amounts.
	Foreclosed Assets and Other Real Estate Investments	OREO 1	All transactions relating to foreclosed assets and real estate investments are complete and timely.
		OREO 2	All foreclosed assets and real estate investments are properly valued.
	Other Assets	ACCD INT 1	Accrued interest receivable is calculated correctly and recorded properly.
		MSR 1	Mortgage Servicing Rights are properly authorized and reflect accurate carrying values.
		BOLI 1	Bank Owned Life Insurance is properly authorized and reflect accurate carrying values.
		GOODWILL 1	Goodwill is properly authorized and reflect accurate carrying values.
		DEF TAX 1	Deferred Tax Asset (or Liability) is properly authorized and reflects accurate values.
	Deposit Accounts	DEP 1	All deposit account transactions are appropriately authorized.
		DEP 2	All deposit account transactions are recorded timely and accurately as to account, amount and period.
		DEP 3	Deposit accounts are maintained properly; review controls effective.
		DEP 4	All deposit account interest rates are appropriately authorized and correctly reflected in rate/index tables.
	E-Channels for Deposit Activity	E-BANK 1	All on-line deposit account transactions are appropriately authorized and accurately executed.
	Accounts Payable	A/P 0	Access to systems utilized for account payable / non-interest expense payment is properly authorized, documented and performed with appropriate segregation of duties. Periodic monitoring of system access is performed and, as applicable, SOC reports are reviewed for control considerations.
		A/P 1	Purchases and payment of non-interest expenses are based on valid approvals.
		A/P 2	Expense coding is appropriately determined and reviewed.
		A/P 3	All disbursements are authorized and accurately posted to the accounting records.
	Other liabilities	PENSION 1	Pension and other compensatory liabilities are accurately stated and changes properly reflected in P&L and AOCI.
		BORROW 0	Access for borrowing or other wholesale funding is properly authorized, documented and performed with appropriate segregation of duties. Periodic monitoring of system access is performed.
		BORROW 1	Wholesale fundings are properly recorded and classified in the accounts.
		BORROW 2	FHLB Borrowings are properly recorded and classified in the accounts.
	Equity and Regulatory Capital	EQUITY 1	All equity and AOCI transactions are properly authorized, recorded on a timely basis and properly classified in the accounts.
	Interest Income & Expense	INT INC 1	Interest income on loans is accurate and complete.
		INT EXP 1	Interest expense on deposit products is accurate and complete.
	Non-Interest Income	NON-INT 1	Non-interest income recognition (Loan Sales) is accurate, timely and complete.
		NON-INT 2	Non-interest income recognition (Insurance Subsidiary) is accurate, timely and complete.
		NON-INT 3	Non-interest income recognition (Investment Services) is accurate, timely and complete.

Princ.	COSO – Financial Statement Linkage	Codification	Financial Reporting Objectives
		NON-INT 4	Non-interest income recognition (Wealth Management) is accurate, timely and complete.
		NON-INT 5	Non-interest income recognition (Unique Lines of Business) is accurate, timely and complete.
	Human Resources / Payroll	PR 0	Access to systems utilized for payroll is properly authorized, documented and performed with appropriate segregation of duties. Periodic monitoring of system access is performed and, as applicable, SOC reports are reviewed for control considerations.
		PR 1	All wages are properly authorized and approved.
		PR 2	All commissions are properly authorized and approved; computations are accurate.
		PR 3	All wage computations are accurate and properly recorded and classified in the accounts.
	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.
11	Technology	TECH 0	Active Directory permissions and access to core system functions are properly authorized, documented and performed with appropriate segregation of duties. Periodic monitoring of system access is performed and, as applicable, SOC reports are reviewed for control considerations.
		TECH 1	Personnel and vendor system access is adequately controlled and monitored.
12	Policies	POLICY 1	Key policies and procedures governing financial reporting are properly articulated and communicated.
13	Relevant Information	REL INFO 1	Spreadsheet reporting precision - information is timely, current, accurate, complete, accessible, protected, and verifiable and retained.
		REL INFO 2	Ancillary system reporting precision - information is timely, current, accurate, complete, accessible, protected, and verifiable and retained.
		REL INFO 3	Custom reports and queries reporting precision - information is timely, current, accurate, complete, accessible, protected, and verifiable and retained.

10 METHODOLOGY – PHASE 1 – PRE-PLANNING

Ahead of the initial field work, we provide Excel template tabs designed to gather/facilitate three items:

Advance document request list

We will provide a list of policies and procedures that we will need to review. A current organization chart and employee listing (names, titles, e-mail) will be requested. A copy of the bank's most current audited financial statements will also be requested. For this, and all documentation requests, we will provide access to our secure portal, for which we deploy Citrix' ShareFile (for your vendor folks to vet/approve, although a service your auditors likely utilize as well).

Bank Profile – Systems and Providers

On a separate tab of the pre-planning workbook, we look to gather information about the systems and providers utilized by the institution. The current list includes:

Primary Regulator
External Audit Firm
Internal Audit Firm
SOX/FDICIA/COSO Testing Firm
Fiscal Year End
Core (Vendor and System)
In-House or Outsourced?
General Ledger
Automated G/L Recon Application
Investment Accounting
ALCO Consulting Firm
ALCO Testing/Validation
Wire Transfers
Daily Balancing
Accounts Payable Processing
Fixed Assets (and Depreciation)
Loan Origination App: Resi Mtg
Loan App: Resi Mtg (On-Line)
Loan Origination App: HELOCS
Loan App: HELOCS (On-Line)
Loan Origination App: Consumer
Loan App: Consumer (On-Line)
Loan Origination App: Commercial
Loan Origination App: Small Business Lending
ALLL/CECL Impairment Tool/Calculator
MSRs Valuation
Derivative Accounting
Payroll
Pension
Bank-Owned Life Insurance (BOLI)
SERP /Deferred/Incent Comp Plans

Walk-Through Sessions

Sessions are planned along functional rather than departmental lines. Since this is a finance-focused project, accounting will have a handful of sessions. Phase 3 speaks to the conduct if these sessions. We typically identify 12 to 15 meetings as follows:

Kick-off - All key dept control owners (See Phase 2)
GL - Acct Admin - Journal Entries - Period Close - Call
Reporting - Fin Statements - MSRs - Inc Tax
Accounts Payable - Fixed Assets
Daily Cash Mgmt - Borrowing - Wires (if finance dept)
Investments – Impairment – Valuation - BOLI
Technology Access Controls – Network – Core – GL - etc
HR - Payroll - Comp – Employee Onboarding
Retail – Branch Capture – Balancing – Checks - Wires
Dep Ops - Wires - Inclearing - ACH - Rate indices – Incoming wire transfers – File maintenance
E-banking - online banking - Remote capture
Residential & Consumer Lending - Loan Servicing - Funding
Commercial Lending – Servicing - Funding
ALLL - Loan Ratings - TDR, Non-accrual
Other (includes non-int. income sources like invest/insurance fees, "captive" operations, etc.).
SEC Reporting (if applicable)

11 METHODOLOGY – PHASE 2 – KICK-OFF MEETING

On the morning of Day One of our fieldwork, we plan an all-hands kick-off meeting to educate, describe the methodology and approach, and most importantly, set the tone. An hour suffices.

COSO Principle 1, focus point 1 leads with:

> ***Sets the Tone at the Top***—*the board of directors and management at all levels of the entity demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.*

Although we continually stress the integrity "message" throughout our work, the kick-off meeting is a moment where we look to executive management to set the tone. The FDICIA/SOX/COSO effort sets a higher standard with regard to a zero tolerance around internal control over financial reporting. Tone at the Top influences the Mood in the Model and the Behavior at the Base.

During the kick-off, our strategy as facilitators is to put the COSO team at ease. We stress that our role is as part of the bank team; and that we are not auditors. Our goal is to capture the way the bank's current control set operates, describe such in the bank's "voice", and offer best-practice additions or change recommendations as applicable.

We go on to describe the process, including walk-through sessions, document requests, review and sign-off steps as described herein. We also help the team understand the eventual testing scope, again emphasizing the zero tolerance standard.

12 METHODOLOGY – PHASE 3 – FUNCTIONAL WALK-THROUGH SESSIONS

Over five or six days on site, we'll facilitate walk-throughs. These meetings are scheduled for 90 minutes each but generally result in 45-60 minutes of controls identification leading to some time remaining to discuss gaps and best practices. From a facilitation standpoint, our preference is to split those days with perhaps a week or so in between, allowing for "catching" all participants (re: vacations) and to allow us time to assimilate the opening sessions, collect documentation and get our work rolling.

For the sessions, we look to have subject-matter experts in the room, and often certain groups might shuffle folks in and out as discussion flows. In all cases, we find it beneficially critical that accounting, risk and internal audit be represented in each meeting if at all possible. Typical projects have seen the Controller and/or CFO in all or most sessions. We've had a couple of projects where the CEO sat in on most sessions with an eye toward best practice; we've had others where we never met the CEO; everyone's culture is different. If the bank has a risk officer and/or internal audit in-house, we find that the perspective brought by those disciplines also add considerable value.

Prep for these meetings is minimal, as we ask that participants arrive ready to walk us through their processes and related control protocols. We do not provide an advance document request list owing to the fact that nuances from bank to bank might be missed if we dictated a "standard" set. Our approach is equal parts discovery and talk therapy as we strive to lead the participants through a self-examination of control processes as we jointly look to identify the "key" control moments.

Guiding our process is our composite consensus controls library, which outlines both the possible and expected controls we might encounter. Our duo approach to these meetings assigns a lead interviewer, leaving the other free to "light-up" the identified controls on our Excel sheet, while each feverishly taking notes.

Following each session, we will provide the bank's COSO team leader / facilitator with a document request list, seeking samples of forms or other auditable evidence to aid our control description drafting.

12-VIRTUAL METHODOLOGY – PHASE 3 – VIRTUAL SESSIONS

In 2020 and 2021, we've all learned to work virtually, and our implementation schedule has adjusted accordingly. Here's the memo we've provided to new clients as we've "adjusted" and a project executed virtually.

COSO Implementation Sessions – Virtual Schedule

Note: Ideally, the Navis guys would like to schedule these sessions in the morning hours, allowing us to collect our thoughts and produce a doc request list "day of" (we will provide project management with access to our secure portal via Citrix Sharefile, with file folders coordinated in a session-by-session order).

Day 1 Kick-off – All hands on deck (60 minutes)
Session w project manager(s) to review the bank's systems (60 minutes)

Day 2 Accounting – GL and Reporting (90 minutes) (if SEC reporting applicable, 120 minutes)
Accounts payable – Fixed assets (90 minutes)

Day 3 Accounting – cash management – borrowing (60 minutes)
Accounting miscellany – deferred tax, pension, goodwill, MSR, FAS 91, etc (60 minutes)
Investments (60 minutes)

Day 4 HR - hiring and payroll (90 minutes)
HR – COSO elements – ethics, whistleblower, performance eval, succession, org, etc (60 minutes)

Day 5 Tech – access controls and "3 lines of defense" conversation for COSO Principle 11 (90 minutes)
Other income sources (investment, insurance, etc) if applicable (30 minutes)

Day 6 Retail – Deposit Ops – E-Banking (treasury services) (30 + 60 + 30 minutes "rolling")

Day 7 Resi lending, operations, servicing, secondary market sales, TDR, impairment (120 minutes)

Day 8 Commercial lending, admin, servicing (75 minutes)
Commercial loan ratings, tracking, review, TDR, impairment, ALLL (75 minutes)

Day 9 Risk and Compliance COSO Elements (COSO principles 6 – 9) (60 minutes)
Pres/CEO "chat" – Integrity, Governance, Succession, Committees (COSO Principles 1 - 5)(60 minutes)

Day 10 Session w project manager(s) to review next steps, including review and sign-off rounds (60 minutes)

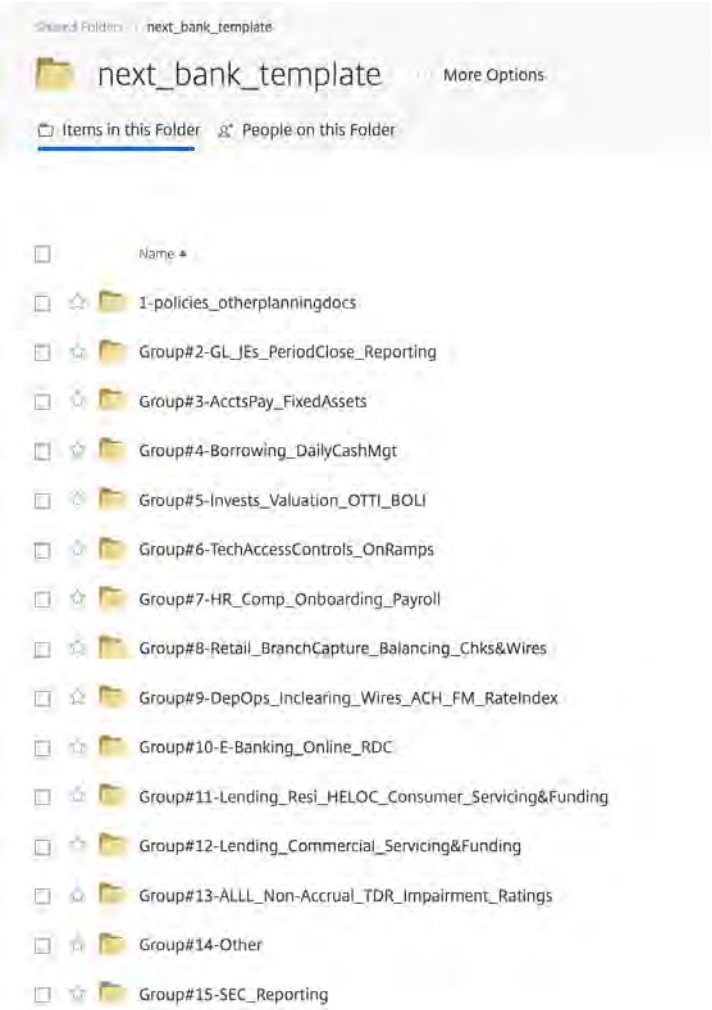
Once sessions are complete Navis awaits docs requested and will require 30 to 45 days (amidst other clients) to turn around the initial ICFR set fully articulated and ready for review.

13 METHODOLOGY – PHASE 4 – DOCUMENTATION REQUEST

As we stated in the phase 3 summary, following each session, we will provide the bank's COSO team leader / facilitator with a document request list, seeking samples of forms or other auditable evidence to aid our control description drafting. The requests may be batched, but will be submitted within a day or three.

We prefer to assign solitary access to our Sharefile secure site to the bank's coordinator, serving as an internal monitor relative to the bank team's response. We set up folders aligning with the walk-through sessions and ask that as the doc request is submitted "codified", that the fulfillment be linked accordingly.

A standard set-up on ShareFile looks like this ….



14 METHODOLOGY – PHASE 5 – INITIAL DRAFT OF CONTROLS

In the sales cycle leading up to these engagements, we like to emphasize that we do all the heavy lifting, unlike many competing providers that merely provide a template designed for the control owners to draft their own control information. We find that multiple competencies and "voices" resulting from a de-centralized approach creates an inconsistent, incomplete, ambiguous, often redundant muddle. By concentrating the drafting of the control descriptions, auditable evidence and other key control elements with experienced hands armed with multiple audit-blessed examples, we can confidently provide an initial draft that meets compliance and audit expectations.

The initial draft commences as document examples roll in (see Project Timeline for relative timing expectations). Our process includes identifying control characteristics (on our controls library tab) and controls details in a more traditional controls matrix format.

The controls library includes an initial assessment as to the following components:

- Reporting Risk If Control Fails (High-Moderate-Low)
- Control Design Guards Against Internal Fraud (Yes-No)
- Control Design Guards Against External Fraud (Yes-No)
- Preventive or Detective
- Manual or Auto / Computer

The standard financial assertions are considered:

- Existence / Occur / Validity
- Completeness
- Valuation / Allocation
- Rights & Obligations
- Presentation/Disclosure

The controls tab captures the following:

- Bank-Specific Codification
- Control Name
- Control Process Narrative
- Control Process Endpoint
- Key Control Considerations
- Key System Dependencies
- Auditable Evidence
- Owner Name
- Task Performer Name
- Frequency
- Annual Sample Size
- Discussion Notes

15 METHODOLOGY – PHASE 6 – CONTROL OWNER(S) DEFINED; ASSIGNED

Who exactly is the control "owner"?

Good question!

If the person performing QC on file maintenance in deposit operations/servicing reports to the deposit ops manager who in turn reports to the COO, who owns the file maintenance review control? The person doing the work, the person supervising the work, or the person responsible if the control fails?

For an initial COSO effort, we like to define the "Task Performer" as the subject matter expert, the person best qualified to describe the process and control protocol, most likely because he/she does it on a daily basis and is thus the best person to edit our initial controls draft to be sure we captured everything correctly. For the "Control Owner", we seek to identify the responsible person, usually at a supervisory level, who is charged with ensuring control processes are adhered to consistently by all staff, and if not, would be entrusted to oversee any remediation efforts. Lastly, when testing commences, the bank may further identify a doc request "go-to" person for providing testing samples, someone who may be other than the Control Owner or Task Performer.

When our initial controls draft is complete, we meet with the bank's COSO coordinator (and other team members as applicable) to assign owners and performers. Our experience finds that this post-control description task serves to more accurately capture the responsible parties versus trying to identify them during our walk-throughs.

Over time, as the COSO effort matures, we find that ownership often shifts to the "do-er", especially as control language is refined after a cycle or two of testing and external audit review.

The control owner will eventually sign-off on each control under their purview.

16 METHODOLOGY – PHASE 7 – CONTROL REVIEW, ASSIMILATION, SIGN-OFF

The review round is the first opportunity for control owners to ponder the completeness of our capture and offer edits. The Excel spreadsheet provides functionality to create a Word "docmerge". By creating a one-page Word-based document for each control, owners needn't be trained on any specific software, merely editing (with change tracking on) the number of control pages owned. The number will vary widely, with the Controller often owning a third or more of the key controls over financial reporting, where, for example, a loan sales specialist may own a solitary control over the booking of secondary market transactions.

Timing is critical to the overall FDICIA/SOX/COSO effort and this step represents a significant variable. We recommend a 2-3 week deadline for review to be completed. We have encountered instances where the bank-side coordinator took weeks to distribute the review docs; instances where the banks offered 5-6 weeks for the review process, and many, many instances of reviews staggering to the finish line months later (4 months may the "record" for review sloth). "Tone" expressed at kick-off and throughout is key, especially with respect to timeliness.

All review documents are loaded up to the ShareFile secure portal.

Once received, we assimilate the changes into the controls matrix, accepting or rejecting edits. Why reject you ask? COSO is completely focused on financial reporting controls, to the exclusion of many compliance considerations such as OFAC, BSA, flood insurance, truth-in-lending, HMDA and so forth. It is common for control owners to offer edits that include compliance related reference. Very commonly, owners reviewing wire controls are hard-wired to include OFAC, offering additional language about the OFAC process as key. Key yes! But not applicable to our myopic COSO focus.

Once all the edits sort themselves out, we move to the sign-off round. Technically this is not a FDICIA requirement, albeit a quarterly SOX requirement. We recommend an annual sign-off by control owners, such that a "roll-up" is created for the benefit of the eventual COSO signers (CEO and CFO). Similar to the review round, response timing is extremely critical to the success of the project. Another docmerge is produced, this time with signature blocks. Curious how sign-off requirements elicit a greater level of scrutiny. This stage is where we really get at control description precision.

17 CONTROLS CONSIDERATIONS - APPLICABILITY

COSO provides a framework for internal controls over financial reporting (ICFR). But, what's truly applicable and what is not?

Entity level qualitative controls confuse this issue quite a bit, as cultural aspects with respect to the "back-drop" against which financial statements are crafted come into play. We speak to that on the "Two Components" page.

But from a purely operational controls stand-point, the issue of applicability is clearer. A question helps frame the debate. *"If this control failed, does it affect the financial reporting of the bank, to the FDIC, in year-end audited statements, or to the SEC?"*

A few examples hopefully serve the cause.

Banks offer safe deposit boxes. Security is key, and controls are widely well articulated and executed in our industry. If security fails, is there a financial reporting risk? Certainly there is a potential liability, but until there is a financial transaction or obligation to be reported, there is no financial reporting risk. Banks do charge for the privilege of safe deposit security. The periodic billing is a financial event to be reported. Applicable, yes. Significant, no. Therefore the significance factor would dictate inclusion or not in the COSO controls matrix.

BSA – One of the most complex and daunting compliance tasks we face as bankers is BSA/AML monitoring and reporting. Controls abound, including internal audits, regulatory audits, SOC-reports and model validation. If BSA compliance is shoddy, the result may be the intake of deposit funds that the bank should not be accepting, or perhaps lurking reporting violations vis-à-vis SARs or CTRs. If however, we accept suspicious funds into a deposit account, as long as the money is recorded and reported the same as any deposit, then we don't have a financial reporting issue. OFAC fits under this example as well as not applicable.

A short list of these and other compliance tasks heavy-laden with control considerations, but not applicable to a financial reporting focus:

- BSA/AML
- OFAC
- Flood Insurance
- Truth-in-Lending
- Good Faith Estimates
- HMDA Reporting

And one last odd non-intuitive example. ALCO. ALCO is a strategy process that guides transaction choices but lies outside of actual execution and reporting. As long as we have well-defined controls for the actual transactions as they occur, we're good.

18 CONTROLS CONSIDERATIONS - SIGNIFICANCE STANDARDS

Significance, for the purpose of identifying key controls over financial reporting, has been traditionally defined in the same manner as financial reporting materiality, with a starting point of "would an error require re-statement" at the "quarterly" level.

However, external audit firms vary on their view of this subject, and the PCAOB, in their oversight role of the external firms, has opinions as well.

Our standards for COSO controls significance follow. Client banks should clear this standard with external audit at the inception of the project.

Almost all accounting estimates and FAS requirements are considered significant including:

- ALLL
- OTTI
- Loan Impairment
- TDR Determination
- FAS 91 (Deferred costs and fees on loans)
- Deferred Tax Asset / Liability
- Goodwill (subject to threshold consideration)
- Mortgage Servicing Rights (subject to threshold consideration)

Significance is further considered with respect to balance sheet and income statement levels / impacts.

Industry best practice has long viewed balance sheet significance at a 1% level. We take a more conservative approach and use a 0.5% level, especially since ALLL, the largest single financial reporting estimate may be less than 1%. The 0.5% level becomes relative with respect to BOLI, goodwill, MSRs, and pension liabilities for example. The 0.5% level, in our opinion, is also more meaningful with respect to the inclusion (or not) of consumer or specialty lending activities.

The income statement metric relies heavily on the re-statement standard expressed above, but as a further metric, we cast potential error levels based on capital ratio levels, a basis-point-of capital approach. As an example, for a bank reaching the FDICIA level of $1 billion, with a 10% capital level, one basis point of capital (tax cushioned at an effective rate of 20%) is $125,000. Banks may choose a more stringent level (perhaps a half basis point). However, if the potential aggregation of errors for a given process or activity is less than $125,000 annually, we consider such insignificant. Consider items such as non-accrual, commissions, sold loan income, other income, RDC underwriting, ACH transactions in this light. We're looking at the error potential, not the expense or income level.

19 CONTROLS CONSIDERATIONS – CONTROL DESIGN ATTRIBUTES

We have identified a list of "ICFR Control Design Considerations" that we capture in our controls matrix. The list seems to grow with every audit, but here are the most prevalent:

Auth-Approval:	The key element of this control is authorization / approval
Review:	Key to this control is explicit evidence of review/acceptance/approval (i.e. more than tacit or verbal; verifiable)
Segregation:	A key element of this control is segregation of duties
Transactional Access:	A key element of this control is restricted access to transactional capability
QC Specificity:	The key element of this QC control is clarity of how the data is verified (i.e. source documents versus specific key fields) – What is the reviewer expected to accomplish?
Competence:	A key element/presumption of this control is competence/experience/training to perform the task
Reconciliations:	Key elements of reconciliation controls are performance/sign-off (inclusive of "clearing" stale items) and review/sign-off
Reasonableness:	The key element of this control is the independent analysis of results for r reasonableness
Policy Review:	The key element for policy review is that the Board (or management) has updated, reviewed and approved with regular frequency (at least annually)
Tech access:	The key element for tech access controls is precision with respect to abilities "turned on" or terminated
Tech access review:	The key element of tech permission reviews is appropriateness of current available access capabilities
SOC:	Key to SOC and SSAE-16-18 control procedures are thorough, competent review and follow-up on user considerations

19.5 MANAGEMENT REVIEW CONTROLS - PRECISION

In As discussed throughout our Playbook, we believe a comprehensive set of ICFRs (Internal Controls over Financial Reporting) are essential for sound management of your institution, not just because FDICIA / SOX compliance might require you to demonstrate you have them (and they work), but also because they can be an effective first line of defense against preventing or detecting material errors or fraud. In a nutshell, a strong internal financial reporting control environment is good for business. Invariably, your internal control set will include a variety of Management Review Controls (MRCs). As the name implies, MRCs are control points that rely on reviews conducted by management of estimates and other kinds of information for reasonableness and to ensure that financial statements do not include any material misstatements. MRCs require significant judgment, knowledge, and experience of management personnel, and to ensure MRCs are operating effectively they mandate consistency in the application of defined threshold tolerances (i.e., level of precision) that might trigger further investigation and resolution of potential reporting errors. Importantly, the level of precision of an MRC should not be seen as an opportunity to nitpick, but rather as a delimiter in assessing whether the control is designed and operating to prevent or detect in timely manner issues that could cause the financial statements to be materially misstated.

Broadly, MRCs encompass just about any material analysis that involves an estimate or judgment; examples include, but are certainly not limited to:

- Budget/actual comparisons of income statement items, where a variance of some percentage and/or dollar amount requires investigation/resolution.
- Month-over-month changes to balance sheet items, again where a variance threshold indicates further investigation/resolution.
- Fair value estimates that rely on management's judgment as to reasonableness.
- Analyses of asset impairment that require both management's judgment as to the reasonableness of inputs (e.g., economic factors or market expectations), as well as documentation of management's conclusions based on assessment of outputs.
- The CFOs final review and sign-off on any periodic statement before filing or inclusion in a Board package.

And remember - MRCs are no different than operational controls. Always always always document the control is performed routinely and consistently via sign-off by the responsible party(ies).

A final word or two about MRCs:

- The PCAOB frequently cites in its inspection reports that a common significant auditing deficiency is the failure to test the design and effectiveness of MRCs that are used to monitor the results of operations. Thus, while you may or may not be a public entity, trust that your external audit firm understands the importance of reviewing your MRCs.
- By definition, MRCs involve comparing recorded amounts with the expectations of reviewers, meaning knowledge and experience are integral to effectiveness. Testing the efficacy of your MRCs includes determination that responsible parties possess the necessary authority and competence to satisfy attainment of control objectives.

20 CONTROLS CONSIDERATIONS – AUDITABLE EVIDENCE

Key to the COSO / FDICIA/ SOX effort is clear identification of the control evidence to be found. We jokingly deploy the **CUSS** method in articulating auditable evidence: **C**lear, **U**nambiguous, **S**uccinct, **S**upportable.

Control descriptions tend to get a bit wordy as they narrate how a given process is controlled, which sometimes contains descriptive language about the process itself and its relation to its pre-process and post- process workflow companions.

However, auditable evidence should be identified in a very straight-forward way.

If, for example, we are considering the order-taking aspect of wire transfers, our control description may recount the process of gathering the customer's information and identification, inputting the information into a system or form; printing the form for customer signature and bank approval; scanning and transmitting to the back office for execution and so forth. Lots of information; lots of detail. But what's the auditable evidence? Pretty straight-forward. Always an official wire transfer form signed by customer and authorized banker. Period.

Specificity regarding auditable evidence minimizes interpretation when testing commences. COSO / FDICIA / SOX represents the only moment in our banking lives that we are empowered to tell an auditor exactly what to test; no more and no less. Testing is an additional cost for any bank reaching the FDICIA or SOX threshold, so clarity equals cost savings.

21 INTRODUCTION TO THE NARRATIVE – QUALITATIVE ASSERTIONS

The FDICIA / SOX / COSO narrative is the capstone to the COSO project. The lengthy document serves to capture the bank's entity-level, cultural, and qualitative controls over financial reporting and more importantly, the environment and culture in which those controls operate.

The assertion document aligns with COSO 2013's 17 principles and 87 focus points.

Following an opening introduction to COSO in general (mostly designed as educational for Boards and Audit Committees), page six begins the task of COSO alignment. COSO's description for each principle and focus point is included (in black font), followed by the bank's assertion in a different font color (typically, we use the bank's logo color). It is important to note that COSO is written for SEC reporting companies and is not banking-industry specific. Therefore, we "answer" some of the COSO guidance at the principle level, and some at the focus point level. Our 55+ COSO projects have been assessed by multiple external audit firms across the country, and we've reached a solid consensus backing this methodology.

The narrative document closes with appendices that list the internal operating controls over financial reporting (ICFR), facilitate executive sign-offs relative to the assertions, and also provide a linkage matrix between COSO and the AFI-CX internal questionnaires (numbers 1 through 4) that most external firms deploy.

The narrative document relies heavily on policies (most notably Ethics and Whistleblower), program documents (especially ERM-related), and committee charters (board and management level). During our initial project focus on departmental operating controls, we are able to gain a sense of the bank's governance structure and culture. Interviews with executive management serve to provide additional information and insight into the bank's unique operating philosophy. Subject overlap from interview to interview is typical and provides some "triangulation" with respect to the bank's culture, reflecting the varying focus and priorities of executive team members.

Our documentation provides a signature page for executive management to acknowledge their review. That said, this a challenging document for management to parse and review. We typically suggest a "first-reviewer", perhaps the CRO, to go through this 70-80 tome with an eye to consistency of policy reference, titles, and such before individual execs give it a read for their own specific content.

22 COSO NARRATIVE INTERVIEWS

During our initial project focus on departmental operating controls, we are able to gain a sense of the bank's governance structure and culture. Interviews with executive management serve to provide additional information and insight into the bank's unique operating philosophy.

A brief description of the nature and objective of the various executive interviews follow. Subject overlap from interview to interview is typical and provides some "triangulation" with respect to the bank's culture, reflecting the varying focus and priorities of executive team members. Preparation and/or advance documentation is not critical to the interviews, as we typically have gathered policies and charter documents in advance.

CEO / President – During an interview with the CEO and/or President (and occasionally inclusive of the bank's Audit Committee Chair if desired by the institution), we explore corporate governance, committee structure, board composition and competency, succession planning, ethics, tone at the top, and whistleblower protocols.

CFO / Controller – The CFO and Controller play a lead role in the process of identifying and articulating key operating controls over financial reporting. The narrative interview serves to "complete the loop" on the project in general. Specific to the narrative, we explore ALCO practices, methodologies, committee structure and standard agenda items. We also explore the qualifications and experience of key accounting personnel.

Human Resources – During an interview with the Head of HR, we explore many of the same cultural issues discussed with the CEO/President. Other subjects include employment practices, performance reviews, and incentives and pressures.

Technology – Tech controls are identified during the operational controls phase of the COSO effort, specifically with respect to system access and permissions. We deploy the "Three Lines of Defense" model in documenting tech's annual processes around IT audit, penetration and intrusion testing, social engineering testing, business continuity and disaster plans, and such. If information security (GLBA) falls under the purview of the IT Director, we would also explore those processes.

Risk – If the Bank has a defined CRO or risk manager position, we would explore risk and fraud issues attendant to COSO principles 6 through 9 with that individual. If the Chief Operating Officer effectively serves such a role, with risk roles reporting to him/her, we would look to include the COO in the interview process. If the risk "machinery" is de-centralized, multiple sessions may be required. Subject matter to be considered in having the right person in the room for those conversations includes BSA, debit card and other fraud processes, vendor risk, and other ERM related processes.

Notably missing from this list are lending, investment, marketing, and retail execs. Their COSO role has largely been fulfilled during the operational controls phase of the project.

23 FDICIA / SOX / COSO PROJECT TIMELINE

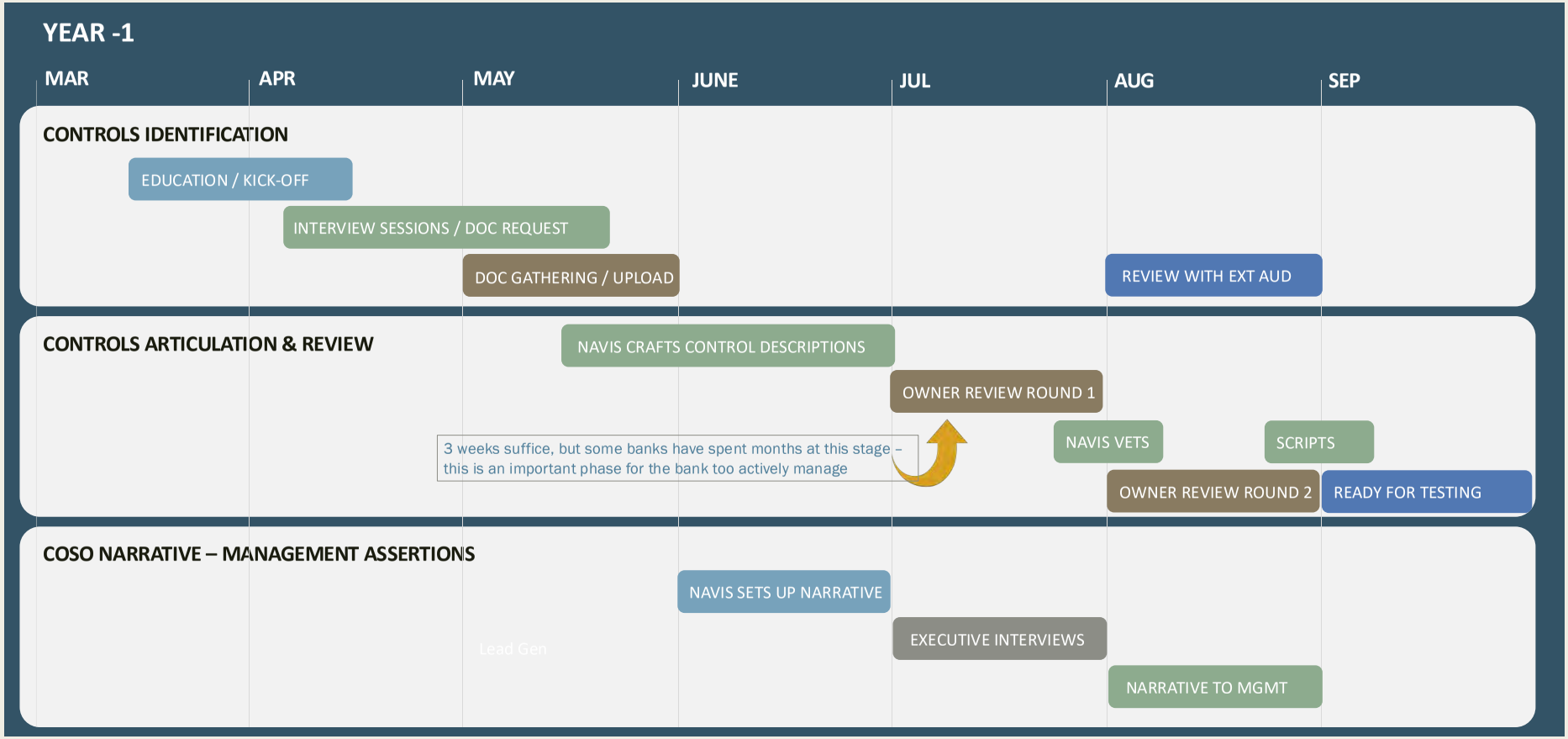
For FDICIA compliance, the measurement date is the fiscal year-end. If a calendar year-end bank's assets exceed $1 billion on 12/31/00, then compliance "begins" on 1/1/01. The timelines that follow depict our facilitation timeline. For the 12/31/00 timing example, this project is best performed early enough in '00 to allow at least one quarter of practice testing ahead of the year of compliance. We find that we are typically kicking off FDICIA projects in Q2 of '00. Banks that have initiated the project a year ahead of time have benefited from additional uptake time to assure that the internal controls over financial reporting are in place and operating as designed. In many cases a "gap" year adds to the practice run-up to compliance.

Once our work is completed, testing commences. Optimally, the "practice" testing occurs. Once into the year of compliance, the bank should absolutely be prepared to have the testing firm engaged and ready to commence testing toward the end of month 6, or early in month 7, such that the first two quarters may be reviewed and feedback provided. Follow-on testing for Q3 and Q4 can then further refine the controls matrix for Year One of compliance, which is always the most fluid in terms of tweaks and corrections.

In our experience the optimal implementation timeline runs approximately 17 to 20 weeks. It is possible to implement in 8-10 weeks "in a pinch". However, we have found in the past few years that proactive adopters don't always fulfill their strategy due to personnel changes, system changes, prioritization issues or other interruptions. Our timelines highlight round one owner reviews as the moment that timing is sometimes stretched. The owner reviews are easily accomplished within three weeks of issue, but often fall prey to distractions of one sort or another. In one instance, 14 months passed between our delivery of the controls drafts and 100% review by all owners.

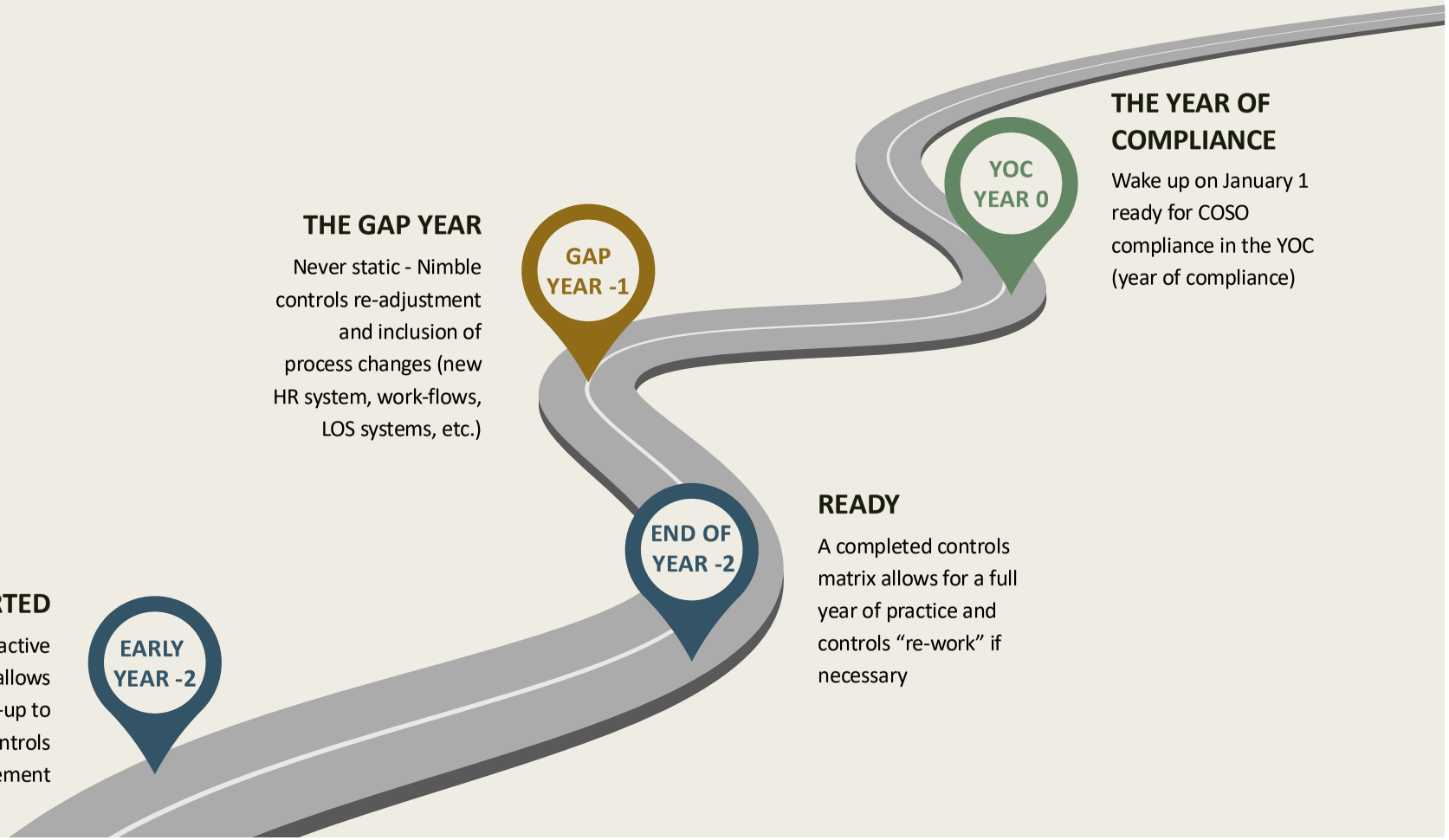
FDICIA / SOX / COSO Implementation

YEAR -1 (or -2): PREPARATION YEAR IN ADVANCE OF COMPLIANCE YEAR (assume calendar year-end)



FDICIA / SOX / COSO Implementation

IF THERE'S A "GAP" YEAR BETWEEN PREPARATION & COMPLIANCE



GETTING STARTED

Proactive implementation allows for a longer run-up to the eventual controls requirement

READY

A completed controls matrix allows for a full year of practice and controls "re-work" if necessary

THE GAP YEAR

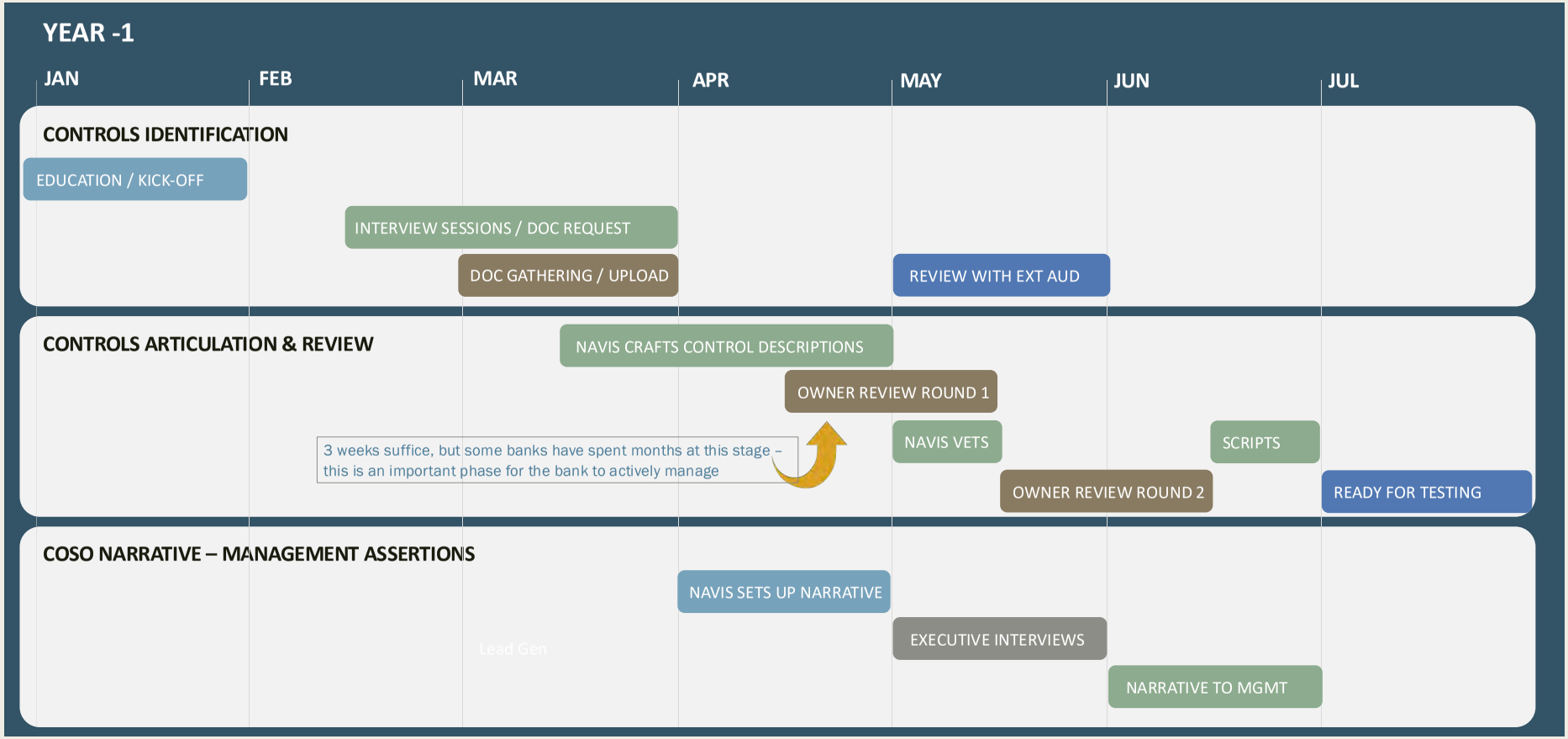
Never static - Nimble controls re-adjustment and inclusion of process changes (new HR system, work-flows, LOS systems, etc.)

THE YEAR OF COMPLIANCE

Wake up on January 1 ready for COSO compliance in the YOC (year of compliance)

FDICIA / SOX / COSO Implementation

YEAR 0: PREPARATION IN THE COMPLIANCE YEAR



24 TESTING – TEST SCRIPTS; TIMING; FEEDBACK LOOP

Test scripts represent docmerge number three in our methodology. Once all the sign-off edits are assimilated, we move to create a multiple page test script to guide the testers.

Controls testing is a key element of FDICIA/SOX/COSO compliance. It is important to note that controls testing is very different from process audits. For example, an internal audit of the wire function is a high risk process dictating annual audit. The wire auditor selects transaction samples by which the entire "voyage" of an individual wire is followed and assessed. For controls testing, we look instead at the control points; wire authorities, wire transfer requests, call-back protocols, not-in-person protocols, wire processing (verification and release). The COSO testing will select a significant sample size (equally out of each quarter) and test the individual control points with a zero tolerance lens. Notable is that each control point will have a unique sample, resulting in the tester looking at 40 different wire requests, then 40 different call-backs, 40 different executions, etc.

A word or two about testing "fails":

- It is often the case that the first year of testing uncovers multiple "fails" of the control description, even if the control is sound. We find that nuances or exceptions within a given control are not always identified in the first go-round (and Murphy's Law tells us that an auditor will always find that one). Details such as additional authorized signers, or alternate e-mail approvals serve as good examples.
- Internal Controls over Financial Reporting (ICFR) are tested with a zero-tolerance outlook. Audit firms tell us that generally only daily or multiple-daily controls may be re-sampled if a fail is identified. Re-sampling is a judgement call, and is often a minimum 50% additional sample set looking for 100% adherence. Clearly if an annual, quarterly, or monthly control fails, the percentage of failure is statistically significant enough to declare the control invalid (at least, as is). Weekly and bi-weekly? Judgment call. In all cases, a search for a remedial or compensating control also kicks in.

SOX testing must be completed each quarter to facilitate the quarterly sign-off expectations of the SEC. FDICIA testing must be sampled "out of" each quarter. A FDICIA institution could (although not recommended) test in month 12 for the entire year, as long as the testing covers all 4 quarters. "Typical" for a new FDICIA bank optimally includes a little bit of a test-testing period. If a bank is proactive in its implementation and gets ahead of its $1 billion year, then having the matrix defined allowing limited practice testing is worth its weight in gold. Once a newly-minted billion bank crosses the threshold, we recommend a 6-3-3 approach whereby initial testing commences in month 6 or 7 looking back at the first 2 quarters. If tweaks are necessary, then 2 subsequent quarterly testing cycles can assure compliance and full absorption of the control changes. Therein lies the feedback loop that is so important in the first go-round. As testers look at the controls for the first time, they are likely to provide a fair dose of control language enhancement, as well as perhaps identify any exceptions to the control rule.

We are often asked about the wisdom of combining COSO testing with the annual internal audit process. We recommend against. We find that the necessary COSO monitoring and "score-boarding" gets muddled when trying to combine those tasks. The problem is not so much with the combined task as it is in maintaining the integrity of COSO monitoring and reporting protocol. Audit firms providing outsourced testing tell us that they will occasionally look to leverage internal audits performed early in the year to perhaps cover the first quarter or two for FDICIA/SOX.

Ask your external firm about their over-sampling philosophy, i.e. how much reliance they will place on the internal testing versus doing their own. We see about a 2/3 over-sample on average.

24.5 TESTING – INDEPENDENCE

We are often asked about the wisdom of combining COSO testing with the annual internal audit process. We recommend against. Audit firms providing outsourced testing tell us that they will occasionally look to leverage internal audits performed early in the year to perhaps cover the first quarter or two for FDICIA/SOX. We find that the necessary COSO monitoring and "score-boarding" gets muddled when trying to combine those tasks. The problem is not so much with the combined task as it is in maintaining the integrity of the COSO monitoring and reporting protocol.

When considering testing independence, it is important in our view to recognize three unique roles:

1) Implementation / update - identifying and articulating the Bank's ICFR set, as well as recommending, refining and designing controls that may not be extant, adequate or auditable. (Navis' role as we assist our family of COSO clients)
2) Testing the control set as specified (Internal Audit and/or outsourced Internal Audit)
3) Opining on the overall scope and methodology deployed, inclusive of over-sampling the internal tests (External Audit serves as the ultimate judge and jury for our combined efforts)

In the proposal stage, we are often asked if we would perform the testing in addition to the implementation. We defer and refer with respect to that option, pointing to internal audit firms we have worked with many many times, and who are familiar with our approach and test scripts. We defer because we view testing on top of implementation to be a conflict of interest (as guided by the AICPA's Code of Professional Conduct) on two counts. Firstly, implementation and update efforts include a large component of control design. We view testing as constituting a review of our own work that at the very least provides an appearance of conflict. Secondly, and perhaps more clear-cut is that the purpose of an implementation or update engagement is a non-audit alignment with the Bank's control owners in which we jointly have a vested interest in the successful outcome of the effort; i.e. successful testing followed by a clean opinion from external.

Over the dozen or more years Navis has provided COSO services, we have often enjoyed the benefit of external audit firms referring us into their clients, with a clear and stated understanding that they are unable to perform implementation services and then provide an attestation opinion. This same ethical line in the sand had also been judiciously observed by internal firms providing the testing attestation, but such has eroded in recent years. On more than one occasion, we have been edged out of engagements by firms crossing this line and offering both implementation and testing.

Editorializing …. We write not so much to criticize but to re-affirm and explain our position that we will not cross that professional barrier and perform testing. It would be simple to hire testers and do so, but harkening back to the premise of this entire effort, COSO opens with Principle1, Integrity "*The organization demonstrates a commitment to integrity and ethical values*" which specifically applies to the "complier", the bank, but then encircles the providers in focus point #11's tenet that segregation is assured inclusive of outsourced service providers. Principle 16 puts the final exclamation point on this discussion referencing: "*The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.*"

25 TESTING – ANNUAL SAMPLE SIZES

Testing sample sizes are subject to review and blessing by the external audit firm. Over the years as banks over-scoped and identified key and secondary controls, the sample matrix allowed for that striation. Similarly, firms allow for multiple attribute controls to be sampled and have an if-then aspect to the required sample sizing.

In our methodology, we strive to maintain a protocol that our controls are single attribute controls. If there are two distinct control points, we define separate controls, not multiple attributes. As such, our controls library results in all single-attribute key controls with no striation or variability attached to the sampling methodology.

The external firms take direction from the PCAOB on this and other aspects of FDICIA/SOX/COSO. In our experience and over the number of banks that we have worked with, we have reached this "composite" sampling matrix:

Frequency of Control	Assumed Population of Control Occurrences	Number of Items to Test
Annual / Existence	1	1
Quarterly or approx 4 occurrences annually	4	2
SEC (SOX) Quarterly - 4 occurrences annually	4	All 4 quarters
Monthly or approx 12 occurrences annually	12	4
Bi-weekly or approx 26 occurrences annually	26	6
Weekly or approx 52 occurrences annually	52	8
Twice weekly or approx 100 occurrences annually	100	12
Thrice weekly or approx 150 occurrences annually	150	18
Daily or approx 250-365 occurrences annually	250	30
Multiple per day	Over 250	40
Variable	TBD	Tester to determine

26 SMARTSHEETS FOR UPDATES & QUARTERLY/ANNUAL CONTROLS CERTIFICATIONS

Once FDICIA/SOX/COSO commences, it never ends. On an annual basis for FDICIA (quarterly for SOX) the matrix should be reviewed by owners and the sign-off and testing process refreshed.

For SOX, testing must occur each quarter; FDICIA testing in subsequent years might follow a 6-3-3 approach (mid-year testing for the first two quarters, followed by testing in the third and fourth quarters), although some banks move to a 6-6 once the process gains maturity.

For FDICIA banks, we find that it's best to wait for audit commentary from the prior year before commencing update. If audited financials "land" approximately 75 days into the new year, starting the update process then assures that testing can occur mid-Q-2. We manage that process for many of our banks, either annually, or with bi-annual check-ups.

Perhaps more critical to the ongoing accuracy and completeness of the COSO matrix is cognizance throughout the organization of changes (people, processes, systems) that have an impact on the identified set of controls. For example, if an institution moves to an Accounts Payable workflow process on February 15 of the new year, the control description needs to reflect the dichotomy of one protocol through that date, and a new protocol from that date forward, directing testers to recognize the modification.

And then we have 2020, and a global pandemic. Regardless of the hardship in having to instantly dial up remote working protocols (that likely never existed anywhere before this) while still functioning as a bank even though we couldn't/wouldn't let anybody into our lobbies so we could all stay safe, FDICIA didn't take a holiday. PPP lending? Loan deferment programs? Sign-offs and approvals completely different looking than what the controls matrix specifies? We all hope these are temporary matters, but don't forget to identify the new controls (or new control language) that will have to be tested to ensure FDICIA compliance.

Commencing in 2020, we moved to Smartsheets for updates and control certifications. The ability to now "work-flow" the cumbersome cycle of review, edit and sign-off provides tremendous time and project-management efficiencies.

Smartsheets work-flows enable an e-mail update form that automatically posts control update language to the matrix for further review/acceptance. Sign-offs performed in this manner result in a documented person/date/time ID that replaces the "create-print-review-edit-sign-scan-upload" loop's inefficiencies.