SOX FDICIA COSO
2013 Best Practices

Presented by:

Raji Sathappan
MBA, CRCM, CAMS, CISA

MERCADIEN

Certified Public Accountants Consultants Wealth Management Technology

Restatements - Mistakes that Dog Financial Reporting

THE WALL STREET JOURNAL.

d U.S. Politics Economy Business Tech Markets Opinion Arts Life

BUSINESS

Bank of America Card Unit Takes $20.3 Billion Regulatory Charge

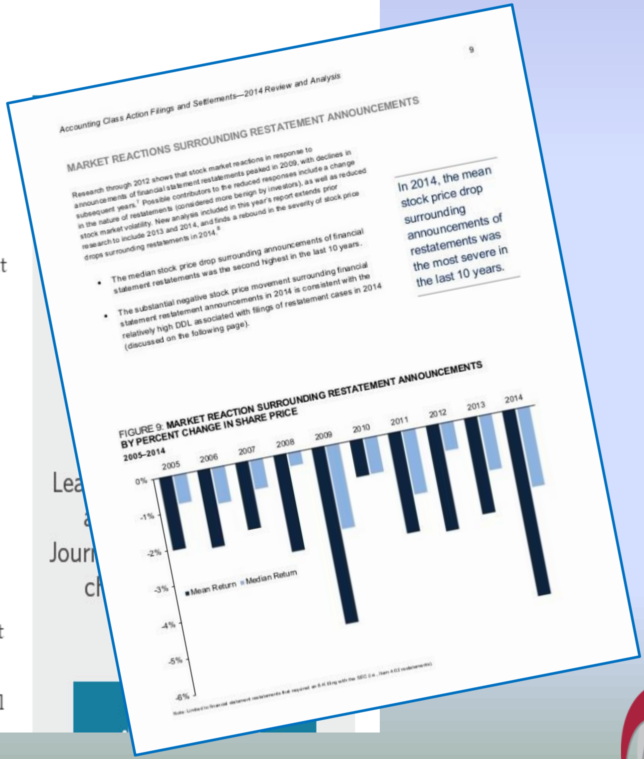
By DAVID BENOIT

Feb. 21, 2011 9:21 p.m. ET

NEW YORK— Bank of America Corp. on Monday said its credit-card subsidiary was restating eight quarters of reports to regulators because it took a $20.3 billion write-down due to deteriorating credit and new regulations over the past two years.

The charge, being taken in "call reports" filed to bank regulators, isn't counted under generally accepted accounting principles, and won't affect the bank's capital or prior earnings. But the enormous size of the charge being reported to regulators shows the extent to which the financial crisis and the regulatory overhaul in its wake have affected Bank of America's card business.

The bank is the nation's largest by assets. The charges announced Monday relate to the bank's FIA Card Services NA unit, which is part of the bank's Global Card Services business. That business' GAAP results aren't impacted by the noncash, non-tax-deductible goodwill


9

Accounting Class Action Filings and Settlements—2014 Review and Analysis

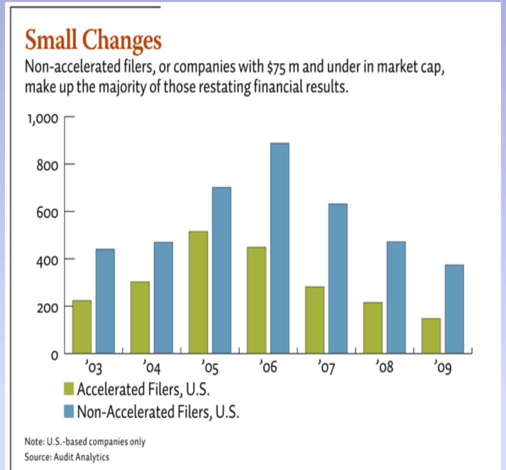
MARKET REACTIONS SURROUNDING RESTATEMENT ANNOUNCEMENTS

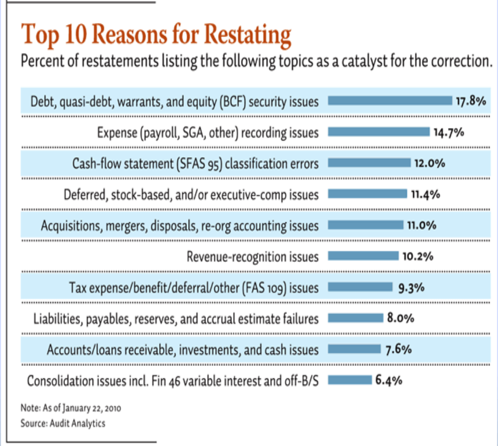
Research through 2012 shows that stock market reactions in response to announcements of financial statement restatements peaked in 2009, with declines in subsequent years.[7] Possible contributors to the reduced responses include a change in the nature of restatements (considered more benign by investors), as well as reduced stock market volatility. New analysis included in this year's report extends prior research to include 2013 and 2014, and finds a rebound in the severity of stock price drops surrounding restatements in 2014.[8]

- The median stock price drop surrounding announcements of financial statement restatements was the second highest in the last 10 years.
- The substantial negative stock price movement surrounding financial statement restatement announcements in 2014 is consistent with the relatively high DDL associated with filings of restatement cases in 2014 (discussed on the following page).

In 2014, the mean stock price drop surrounding announcements of restatements was the most severe in the last 10 years.

FIGURE 9: MARKET REACTION SURROUNDING RESTATEMENT ANNOUNCEMENTS BY PERCENT CHANGE IN SHARE PRICE
2005–2014





MERCADIEN

Agenda

- What do the Docs Look Like?
- FDICIA – Safety and Soundness
- SOX – ICFR
- COSO 2013 – the Language of Controls
- Scoping and Process Mapping
- Control Testing
- Tips and Tricks

So What Does This Look Like?

- Scoping and Materiality Document (IS and BS materiality thresholds)
  - All processes risk-rated – Implications to type of testing
- Internal Controls Questionnaire
- EWC (hang your hat on controls)
- Process Narrative
- Risk and Controls Framework
- Test Plan for Key Controls
  - Key Control = Litmus test?
- ICD Gap Log
- S 302 Sub-certification
- S 404 Certification (snapshot of point in time)

MERCADIEN

FDICIA in a Nutshell

- **Who?** Banks with assets > $1 billion to assert internal control methodology in place to assure integrity of annual audited financial statements, as well as four quarterly Call Reports.
  - Measurement date for asset size is fiscal year-end, necessitating compliance following year.
  - If asset size > or = to $500 million but < $1 billion, only assessment of ICFR and compliance with laws required. Section 362.2 (b) (1) (2).

- **When?** Annual report on internal controls. Must evaluate controls on yearly basis for as long as you meet the requirements.

- **What?** Control design AND operating effectiveness.

FDICIA vs SOX

- SOX (Sarbanes-Oxley Act of 2002) is **non-industry specific** compliance requirement for all SEC registrants (Q and K filers).

- SOX born in Enron era. Measure for required compliance is market cap of $75 million (level accelerated filer status attained). Measurement date for capitalization levels is June 30, necessitating compliance in fiscal year ending after such date. SOX compliance extends scope of financial reporting to include **quarterly** filings (but currently not proxy information). Modeled after FDICIA (specifically, rule 112).

- Both require management and EA **annual** evaluation and reporting.

Key Differences: FDICIA vs SOX

1. Scope

- FDICIA is broader, relates to internal controls over operating efficiency, financial reporting and compliance with laws and regulations.

- SOX Section 404 relates to ICFR only.

Key Differences: FDICIA vs SOX

2. Reporting

- FDICIA requires reports filed with FDIC and institution’s primary regulator. SOX 404 requires both management’s assertion and auditor’s attestation, including any material weaknesses identified, be publicly disclosed in annual report.

- Publicly-traded financial institutions with assets > $1 billion subject to both requirements. Institutions with assets > $1 billion, but privately-traded, subject to FDICIA 112 only. Publicly-traded institutions with assets < $1 billion subject to SOX 404 only and not 112.

- Privately-traded financial institutions with assets < $1 billion subject to neither regulation.

Mercadien

FDICIA vs SOX vs COSO

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

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

- In 2013, COSO rolled out an updated document that took effect 12/15/14.

MERCADIEN

Why COSO 2013?

- Framework reflects considerations of many changes in business, operating and regulatory environments over past several decades, including:
    - Expectations for governance oversight
    - Globalization of markets and operations
    - Changes and greater complexity in business
    - Demands and complexities in laws, rules, regulations, and standards
    - Expectations for competencies and accountabilities
    - Use of, and reliance on, evolving technologies
    - Expectations relating to preventing and detecting fraud

Mercadien

COSO 2013 : Evolution

Original Framework	COSO's Internal Control – Integrated Framework (1992 Edition)
Enhancement Objectives	Address Significant Changes to the Business Environment and Associated Risks; Codify Criteria Used in the Development and Assessment of Internal Control; Increase Focus on Operations, Compliance and Non-Financial Reporting Objectives
Key Changes	Updated, Enhanced and Clarified Framework; 17 Principles Aligned with 5 Components of Internal Control; Expanded Internal and Non-Financial Reporting Guidance
Updated Framework	COSO'S Internal Control – Integrated Framework (2013 Edition)

MERCADIEN

Internal Control Oversight-COSO Model

- **Control Environment –** Establish integrity and ethical values, oversight structures, authority and responsibility, expectations of competence and accountability to the board.

- **Risk Assessment –** Oversee management's assessment of risks to achievement of objectives, including potential impact of significant changes, fraud and management override of internal control.

Internal Control Oversight- COSO Model

- **Control Activities** – Provide oversight to senior management in development and performance of control activities.

- **Information and Communication** – Analyze and discuss information relating to entity’s achievement of objectives.

- **Monitoring Activities** – Assess and oversee nature and scope of monitoring activities and management’s evaluation and remediation of deficiencies.

COSO 2013

- There is value in mapping existing controls to the 17 principles.
  - Companies must demonstrate that 17 principles are present.
  - 87 points of focus can be used as guide, are not required.
- Ensure that fraud risk assessment included in overall risk assessment activities. Can be embedded or separate.
- COSO 2013 still requires top-down, risk-based approach. New COSO not intended for use as checklist.
- Take reasonable approach; don't over-engineer. COSO 2013 is about review and enhancement of internal controls using continuous improvement mindset.

MERCADIEN

COSO 2013 – Go Live Date

- Timeline for implementation.

- The original Framework will remain available and deemed appropriate for use through 12/15/14, giving entities ample time to make the transition.

- According to COSO, continued use of original Framework during transition period is acceptable.

MERCADIEN

Why Scope?

- Project plan that will be given to auditors and audit committee, a roadmap to compliance.
- Addresses timing, staffing, COSO framework implementation, testing level, control environment and identification of significant systems.
- All significant processes drive FS.
- Align with IA universe.
- Assign ownership.

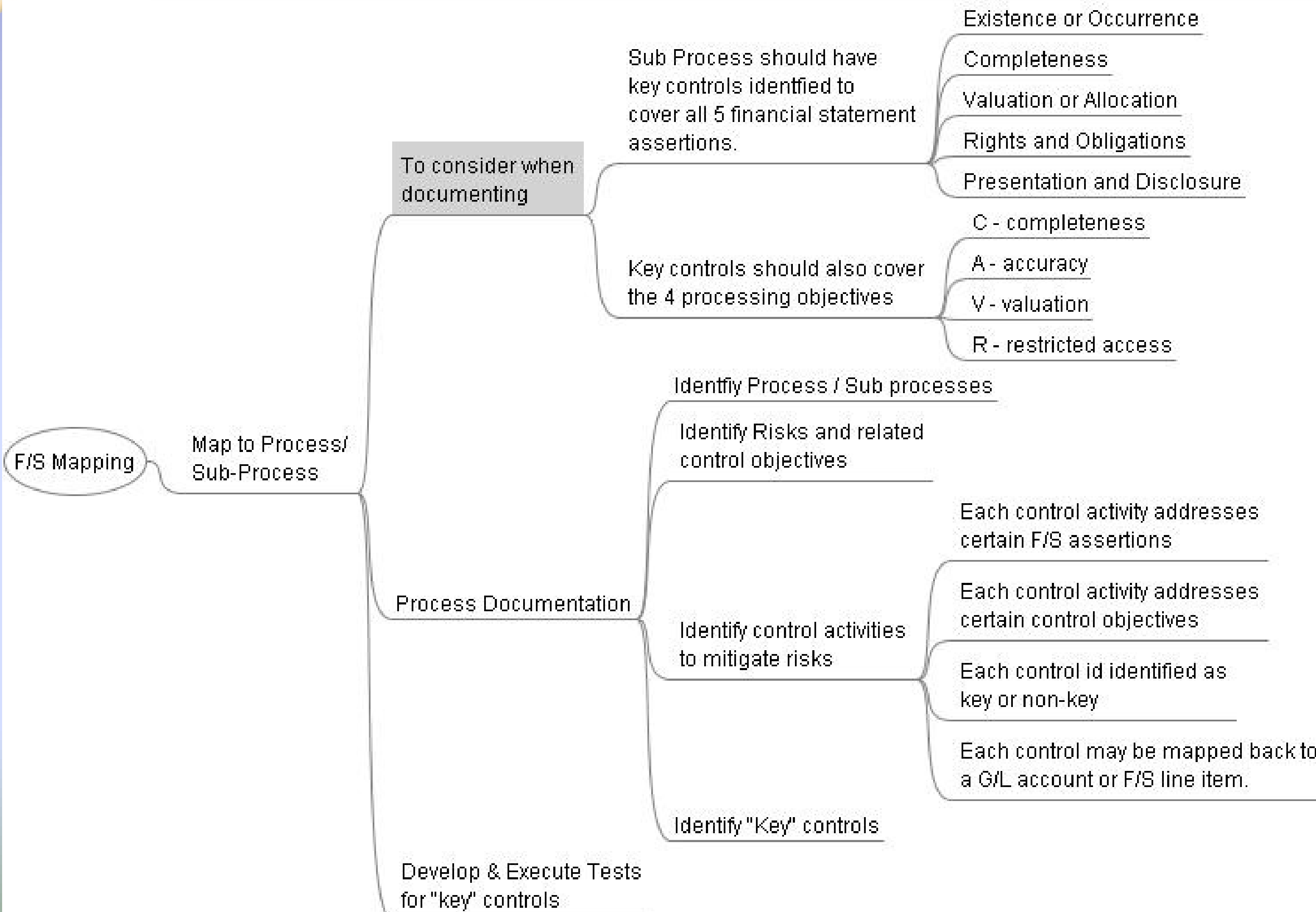
MERCADIEN

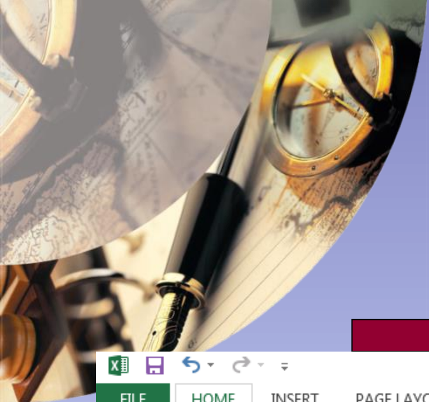
SOX Mapping – AS 5

- Work from Latest BS and IS.
- Identify significant accounts and disclosures.
- Identify significant business units and locations.
- Indicate relevant financial statement assertions.
- Determine major classes of transactions.
- Document significant processes and sub-processes.
- Note IT infrastructure.
- Identify internal controls over major classes of transactions.
- Evaluate likelihood, magnitude and other controls.
- Determine which controls should be tested.

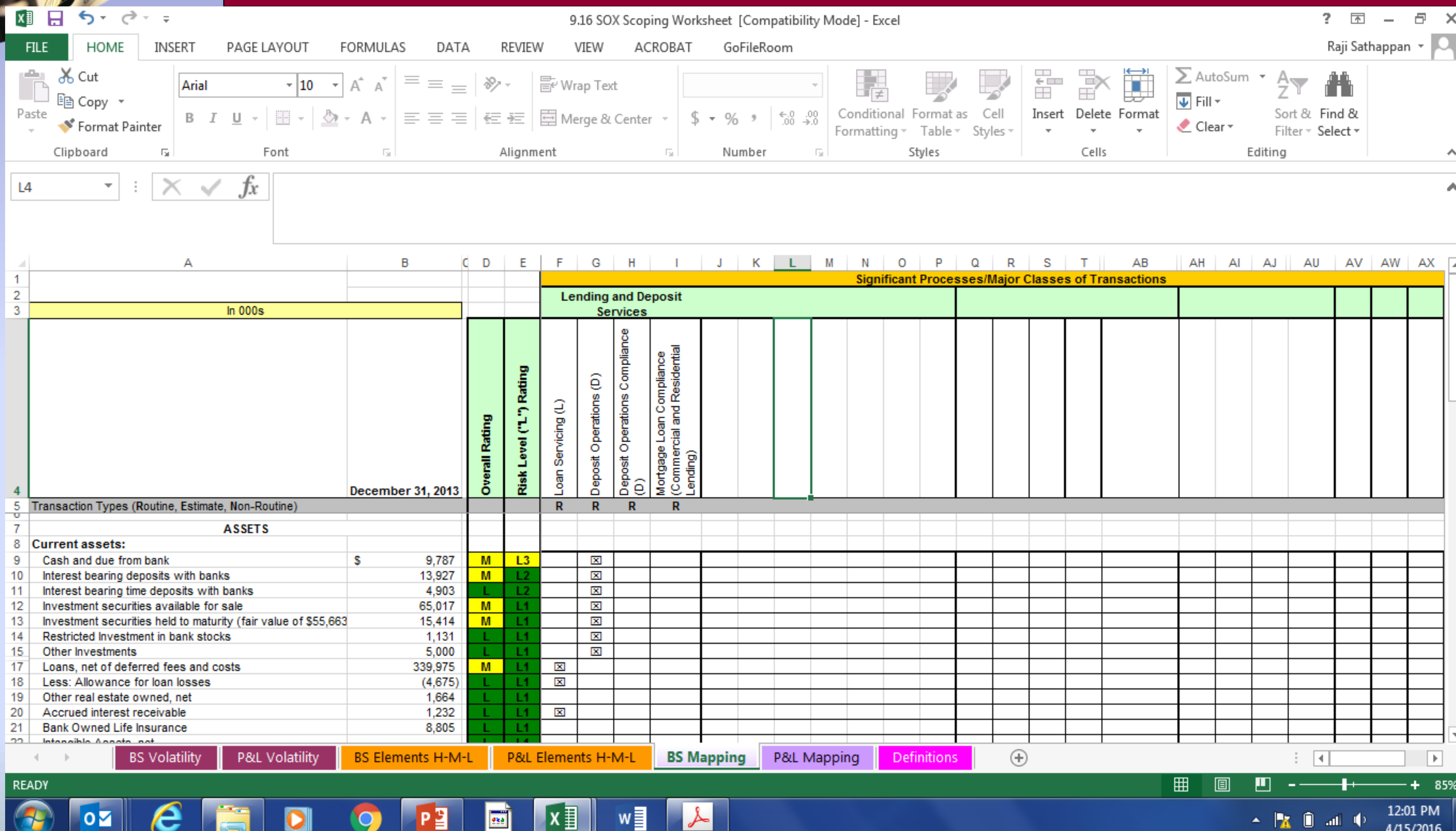
Mercadien

Example of Scoping/Mapping





Snapshot of SOX/FDICIA Mapping



9.16 SOX Scoping Worksheet [Compatibility Mode] - Excel

Significant Processes/Major Classes of Transactions

Lending and Deposit Services

In 000s	December 31, 2013	Overall Rating	Risk Level ("L") Rating	Loan Servicing (L)	Deposit Operations (D)	Deposit Operations Compliance (D)	Mortgage Loan Compliance (Commercial and Residential Lending)
Transaction Types (Routine, Estimate, Non-Routine)				R	R	R	R
ASSETS							
Current assets:							
Cash and due from bank	$ 9,787	M	L3		☒		
Interest bearing deposits with banks	13,927	M	L2		☒		
Interest bearing time deposits with banks	4,903	L	L2		☒		
Investment securities available for sale	65,017	M	L1		☒		
Investment securities held to maturity (fair value of $55,663	15,414	M	L1		☒		
Restricted Investment in bank stocks	1,131	L	L1		☒		
Other Investments	5,000	L	L1		☒		
Loans, net of deferred fees and costs	339,975	M	L1	☒			
Less: Allowance for loan losses	(4,675)	L	L1	☒			
Other real estate owned, net	1,664	L	L1				
Accrued interest receivable	1,232	L	L1	☒			
Bank Owned Life Insurance	8,805	L	L1				

BS Volatility | P&L Volatility | BS Elements H-M-L | P&L Elements H-M-L | BS Mapping | P&L Mapping | Definitions

MERCADIEN

Independent Audit Committee

- SOX requires all Audit Committee members to be independent directors (including a financial expert) and to serve as primary liaison between company’s accountants and Board.
- Consider appointing at least one Audit Committee member who is a financial expert and can question and communicate effectively with outside accountants and auditors.
- Adopting SOX-compliant best practices in this area sends strong message to investment community regarding your financial and ethical position.
- Adopting an Audit Committee charter that mirrors these requirements is considered best practice and may be required by lenders or outside accountants.
- The lack of independent Audit Committee could be raised by a plaintiff’s attorney in the event of a claim of financial mismanagement or fraud.

Independent Audit Committee
(cont'd)

- Simply forming an independent Audit Committee not sufficient to protection.
- Audit Committee must appreciate large and complex financial risks taken and identify the key judgments made by management and external accountants in preparing the financial statements.
- To be effective, Audit Committees should ask external accountants/auditors for specific information concerning:
  - repeatedly occurring transactions
  - material items where accounting literature allows alternative methods of presentation
  - material differences in significant accounting policies between the company and main competitors

Audit vs Test

- Mission of tester is not to re-audit whether the transaction is correct.
- Mission is to test if controls are ***sacredly*** **deployed.**
- Differences between internal audit and controls testing.

MERCADIEN

Key Controls Only – Risk Weighted

- The Risk Rating Scale has to be clear.
- If control fails, here's a handy scale to measure your CEO's reaction.

L = Laid Back.
Don't really care

M =Mad, Miffed

H = Hot, Horrified

Testing OE

- Testing Operating Effectiveness, also called Activity Level Controls.
- Includes testing of expenditures, treasury, revenue, payroll, property, debt/equity, etc.
- Activity-level control tests should be tested after controls are re-designed. Company must be sensitive to sustainability aspect of SOX 404, so activity-level control testing should not be completely ignored at outset. Conversely, documenting activity-level control tests before addressing design deficiencies leads to redundancy, because controls will need to be retested after the redesign.

MERCADIEN

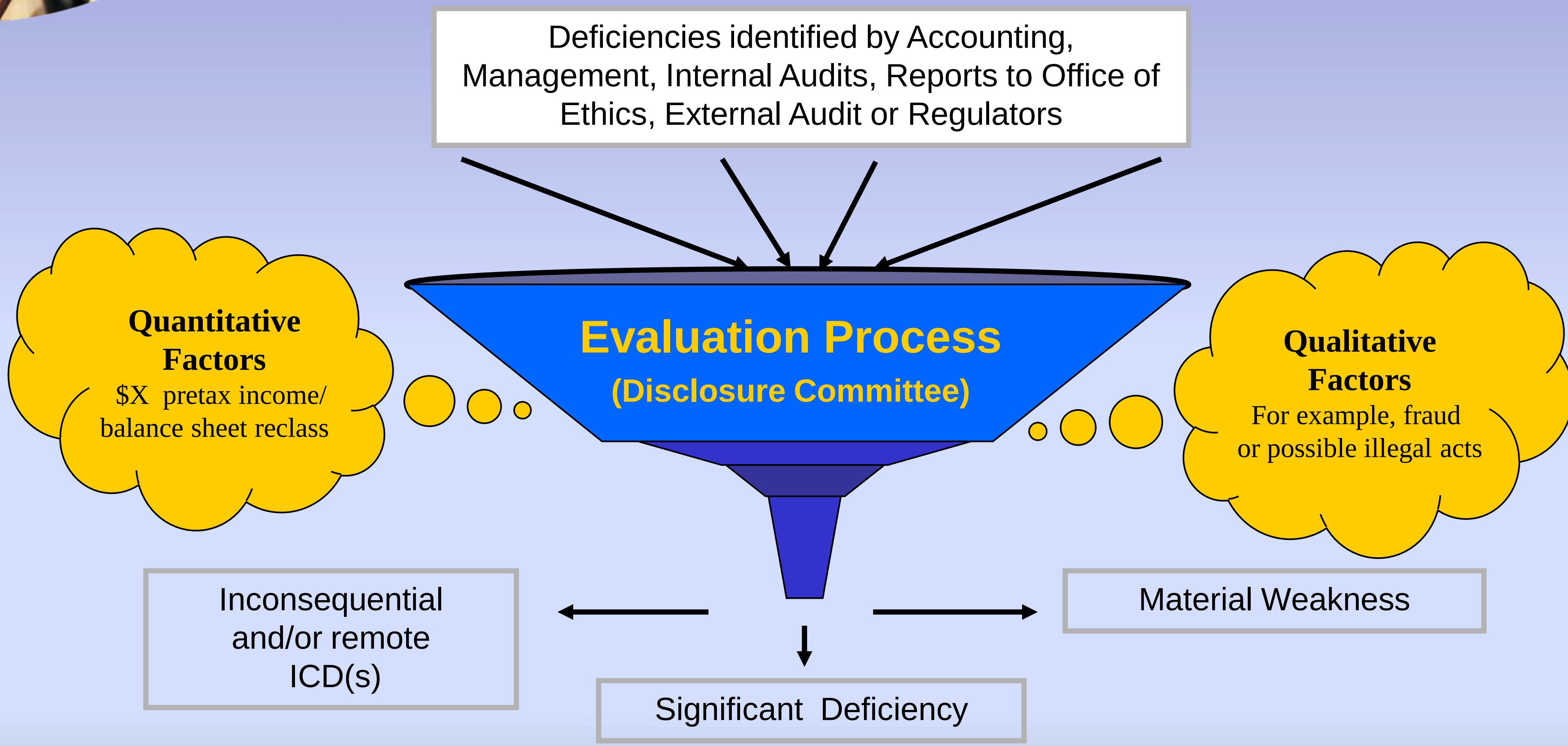
IT Controls

- General IT controls (user access-EWC) and App controls (embedded in process controls) and design of IT environment.

- IT should be assessed concurrently with other tests, including IT risk assessment process.

- 2 areas need to be tested and documented in the area of IT - general computer controls and application controls.

Internal Control Deficiency Evaluation



OUTPUTS = Labeled Deficiencies

Internal Control Deficiency Evaluation

Sources of Internal Control Deficiencies & Disclosure

- Control Owner certification
- Control Executive verification
- Internal Audit validation of control design and effectiveness
- Internal Audits
- External Audits
- Accounting errors identified via closing process
- Other process/control evaluations by internal or external parties
- Regulatory financial reviews
- Ethics hotline

Initial Discussion of Impact

Pre-Disclosure

List of all deficiencies and recommendation of impact of such

Disclosure Approval

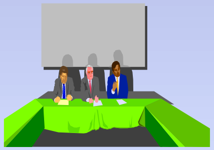
Disclosure Committee

Management determination of deficiency impact & external disclosures

Disclosure Review

Sr. Leadership

Review to support annual & quarterly certifications (CEO & CFO) & 10K/Q disclosures



Audit Committee

Review of management determination of deficiency impact & external disclosures

MERCADIEN

In Summary

Tips and Tricks

10 Steps to Implement SOX 404 Project

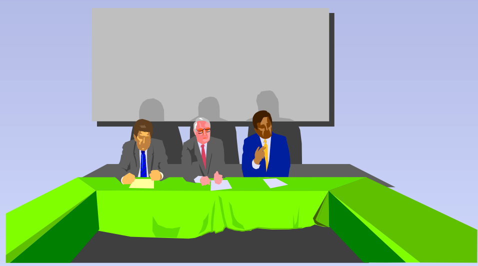
MERCADIEN

Best Practices

- Governance Structure
- Roles and Responsibilities
- Implementation Approach
- Implementation Discipline
- Program Fundamentals
- Program Infrastructure

Governance Structure

Executive Sponsor: EVP



Audit Committee

Report to AC periodically
on progress of project

Program Oversight

*Approach/Methodology
**Program documentation

Steering Committee

Eg: Meet 3 times – project
inception, mid-point and
end of project

Program Oversight

*Approach/Methodology
*Rollout
*Scope
•*Program documentation

Business Working Group

Meet weekly to discuss project deliverables
And execution. Deliver project deliverables
to external auditors

Responsible for

- Approach/Methodology
- Rollout
- Scope
- Program documentation

MERCADIEN

Roles & Responsibilities

Steering Committee & Working Groups	Program oversight and governance decisions (e.g., scope, approach, roles and responsibilities, etc.).
Program Management Office (PMO)	Program administration including coordination/support, ensuring all parties are carrying out responsibilities, reporting and analysis.
Control Owner	Periodic certification (self-assessment) of control performance.
Control Executive	Approval of control design and periodic verification of control.
Support Management	Assists Executives / Owners with responsibilities.
Internal Audit	Periodic assessment of control design and performance.

Devising Your Governance Model

- There is no <u>one</u> right model.

- The right model is dependent on the following environmental factors:
    - Industry
    - Company Structure
    - Management Philosophy (Centralized vs. Decentralized)
    - Company Size and Complexity

Implementation Approach

Define Methodology & Scope
Establish Governance Structure & Program

Monitor Program Methodology & Scope

Document Process & Controls

COSO
Entity Level Controls

Corporate Processes
Investments, Finance, HR, Legal

Business Unit Processes
Lending, Collateral Valuation, etc.

IT Processes
Application and general controls

Processes are across Corporate, Business Units and IT functions. Also includes entity level controls, compliance and statutory reporting controls. As areas are documented, control design is agreed upon by the Area Executive and Controllership. Owner certification (self-assessment) begins upon agreement of control description and attendance at New Control Owner training.

Phased Program Commencement – Document 5 processes
Owner Certification, Executive Verification & Internal Audit Testing

ICD Prioritization & Remediation
Pre-Screen, Risk Rank, Prioritize, Commit Resources, Remediate & Validate

Document and Test Remaining Processes

Communication & Training to Governance Groups, Control Executives, Control Owners, Internal Audit and other impacted parties….

MERCADIEN

Implementation Discipline
6 Key Processes

Gate 1
Scheduled
- **Interview Owner**

Gate 2
Drafted
- **Document Walkthrough Narrative and RCM**

Gate 3
Approved
- **PMO and McGladrey**

Documentation & Locking in Control Design

Gate 4
Testing
- **PMO approval**

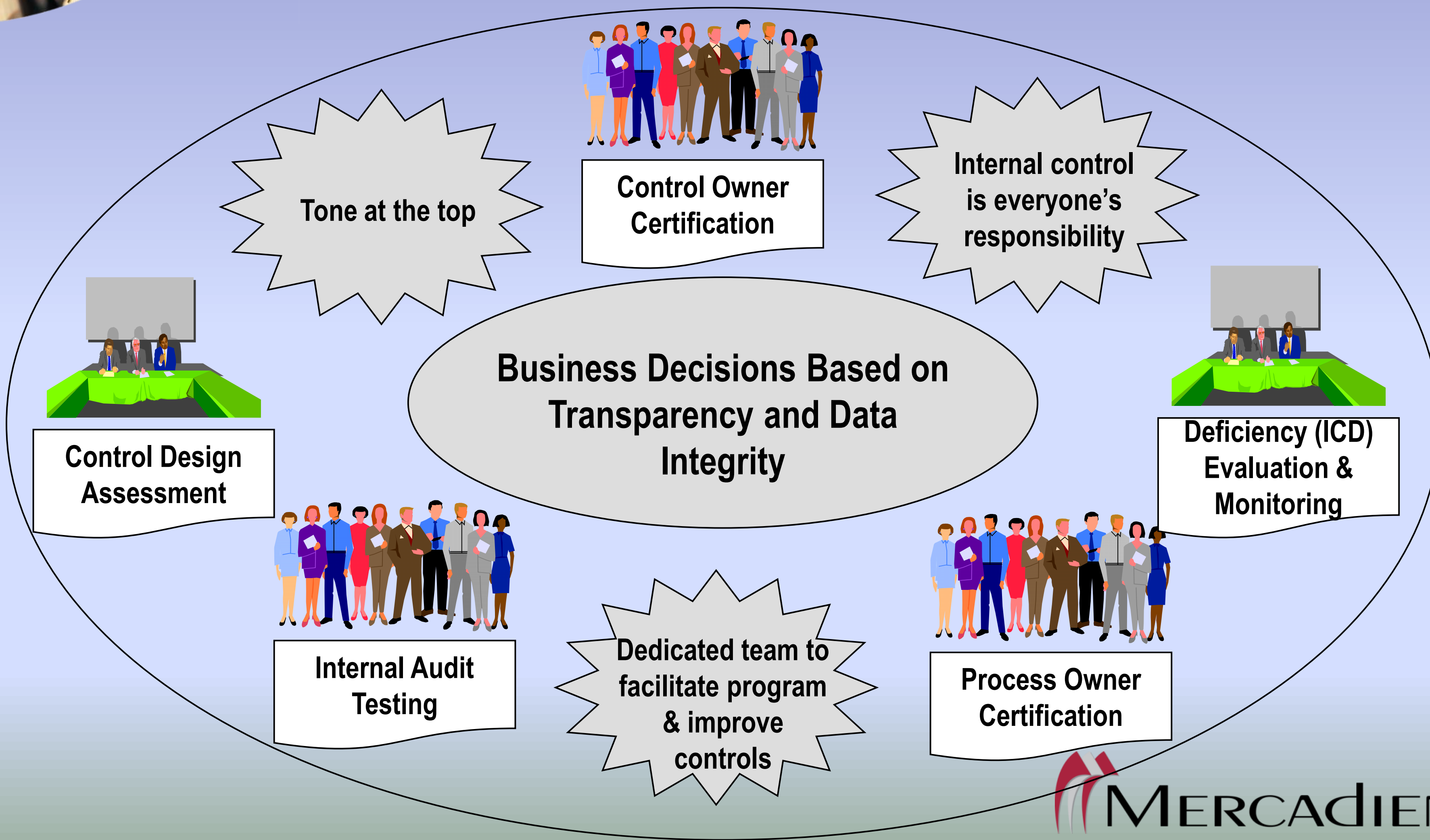
Gate 5
Certification
Process Owner

Gate 6
Remediation
- **Process owner and PMO**

Assessing Control Performance

MERCADIEN

Program Fundamentals



MERCADIEN

Program Infrastructure

- Single repository to document key controls, including:
  - COSO (entity level) controls
  - Business process controls
  - IT controls (application, general)
- Risk and Control Matrix (RCM) also facilitates:
  - Assessment of control design - key controls to support related relevant assertions of significant financial statement accounts and line items.
  - Assessment of control performance
  - Recording and monitoring of identified deficiencies
- Most responsibilities run a quarterly cycle

Program Infrastructure

- Training – who does what.
- What does it mean to be project leader, process owner, etc.?
- Tester – Keep it independent so EA can leverage bank’s testing info – reduced fees.
- Black and Blue excel SS – EA and IA SOX team QC.
- Doc Gaps – Systemic breakdown vs Isolated incidence.
- Soak period.

Mercadien

Program Infrastructure

- Include EA in project plan and keep them in the loop:
  - Communicate, communicate, communicate.
  - External and their qualifications, in-house team and their resumes.
  - Include outside auditors in control concepts, but not testing.
  - Ensure management and upper management are on board.
  - Prepare audit committee.
  - Expect much improvement and redesign in year 1. Debrief and retune.

- It is also wise to coordinate and determine what constitutes a significant control with outside auditors to minimize both over- and under testing.

- Use what you have - leverage.

MERCADIEN

COSO Best Practices

- Facilitate broad awareness across company of new COSO Framework:
  - Ensure adequate tone at top and buy-in to Framework’s value.
  - Make sure there is control ownership and accountability by management.
  - Align expectations with external auditors.
  - Underscore that stronger corporate governance translates into stronger business results and increased shareholder value.
  - Consider expanded use of updated Framework for operational and compliance areas where internal control failure could significantly impact business results.

Think About This!

- Your company’s stage of growth and financial ability to become SOX-compliant.
- Your industry and SOX-related requirements of companies with which you do business.
- Your timeline for becoming SOX-compliant in the context of potential IPO, merger or acquisition.
- The culture and personality of your business when adopting a Code of Business Conduct and Ethics.
- Weight of potential costs associated with appointing independent directors vs benefits they will provide to your company.
- Paying more to financial experts serving on your Audit Committee.
- Compliance with SOX provisions has become best practice among many private companies and is often expected by third parties you may want to do business with.

MERCADIEN

Think About This!
(cont'd)

- Full compliance with all requirements costly and time-consuming; private companies can choose most helpful practices.
- Adopting certain policies such as ethics codes, whistle-blowing policies not costly, involve one-time upfront expenses.
- Other practices such as hiring independent directors can be costly; many potential directors will require purchase of expensive D&O insurance.
- Despite varying costs, once implemented, best practices can strengthen operations, efficiency, reputation and add value, particularly toward acquisition exit-strategy.
- Private companies have benefit of adopting a hybrid approach and choosing best provisions to implement.

Think About This!

(cont'd)

- SOX-compliant best practices are important to consider when planning to go public or if become acquisition target.

    - Third-parties, such as investors and insurers, may insist on SOX compliant internal controls and best practices.
    - They may be required for certain state and federal contract eligibility.
    - Potential high-quality board members may be reluctant to serve without them.
    - They give a better chance of avoiding or successfully defending against litigation.

Questions?

Contact:

Raji Sathappan, MBA, CRCM, CAMS, CISA

Director, Financial Institutions Services Group

rsathappan@mercadien.com | 609-689-9700

MERCADIEN