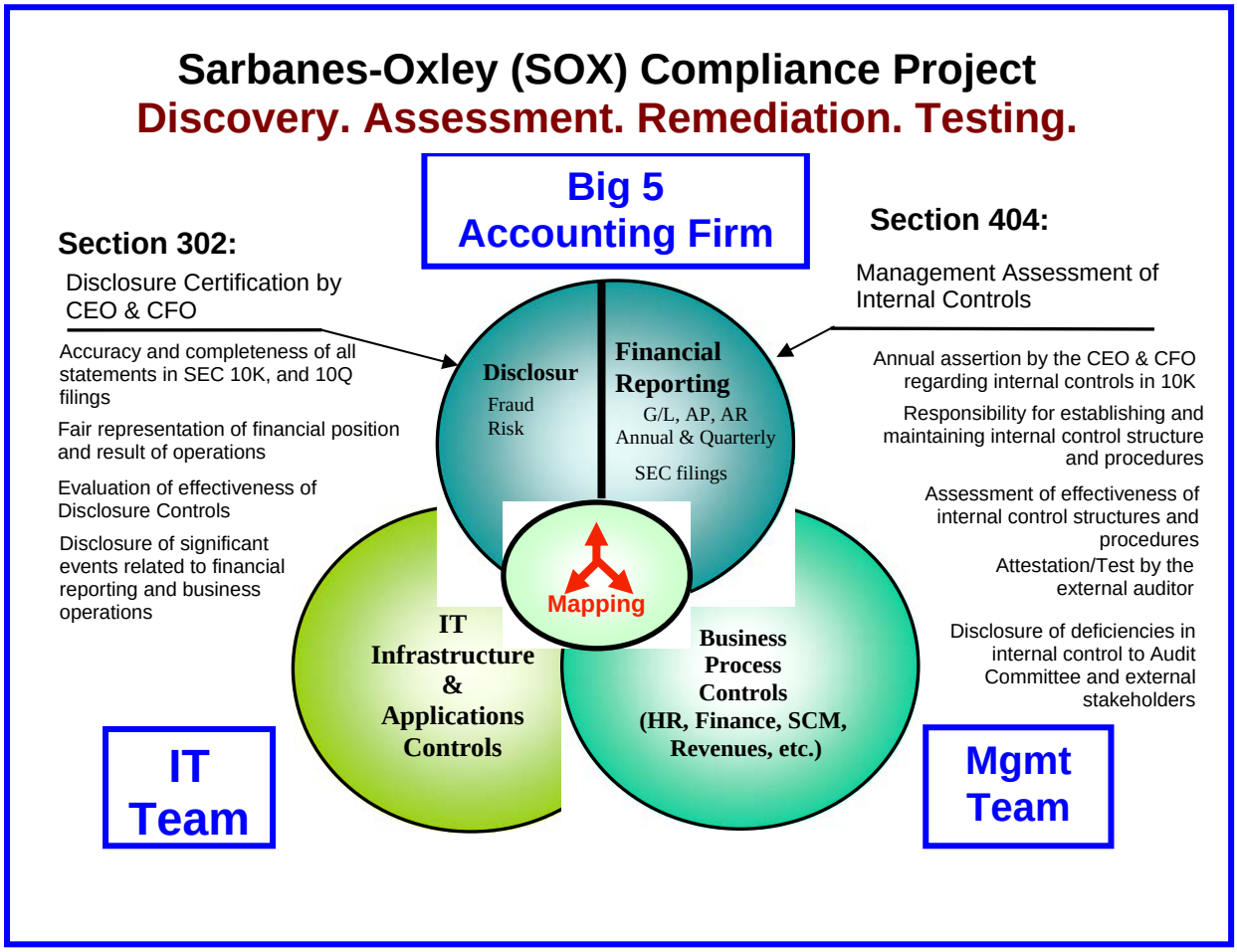
International Institute of Management (EJ) Executive Journal

IIM – Best Practices Paper

CIO and Sarbanes Oxley (SOX)
Corporate governance best practices

What is Sarbanes-Oxley (SOX)?

- SOX act of 2002 is a US government regulation that establishes requirements for public companies and their executives to implement test and maintain internal controls of financial reporting. SOX compliance requires internal policies, procedures and controls to "provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the company's assets that could have a material effect on the financial statements."
- "Internal control" requirements are achieved by integrating, documenting and testing three main enterprise functional areas, these are Financial Reporting, IT Security and Business Process controls (as shown in the figure below).



International Institute of Management (EJ) Executive Journal

What is COSO & COBIT?

- The SOX act recommends the use of COSO (The Committee of Sponsoring Organizations of the Treadway Commission) as the framework for auditing financial systems.
- The Committee of Sponsoring Organizations (COSO) was formed by several professional groups, including the Institute of Internal Auditors (IIA), Financial Executives Institute (FEI), American Institute of Certified Public Accountants (AICPA), American Accounting Association (AAA), and Institute of Management Accountants (IMA).
- The COSO Report, as the framework became known, was the first-ever attempt in corporate America to establish a universal definition of internal control, along with proposed guidelines for governance, independence and quality assurance.
- The Information Systems Audit and Control Association (ISACA) has prepared an industry accepted "mapping" of CoBIT (Control Objectives of Information and Its related Technology) to the COSO internal control model and the S-OX information system internal control requirements.
- While CoBIT has a much broader scope in the audit process, INS core competencies align directly to the development of the support systems, processes, procedures, and controls identified under the GCCs (General Computing Controls.) . The GCCs include controls for:
    - Software (Systems) Development Lifecycle (SDLC)
    - Change Management
    - Production Operations
    - Operations Security (Access and Vulnerability Management)
    - Systems Backup and Recovery
- Specifically CoBIT focuses on the following internal control processes:
    - Acquiring or developing application system software
    - Acquiring technology infrastructure
    - Developing and maintaining policies and procedures
    - Installing and testing application software and technology infrastructure
    - Managing changes
    - Defining and managing service levels
    - Managing third-party services
    - Ensuring systems security
    - Managing the configuration
    - Managing problems and incidents
    - Managing data
    - Managing operations

International Institute of Management (EJ) Executive Journal

What is SOX compliance project methodology and timeline?

SOX compliance is a program that includes multiple projects with typically 3 main players; an accounting audit firm, an IT security firm and the client's business process management team.

A Typical Project Methodology and Timeline

Phase 1 Discovery

- Business Scope Identification, Project Plan and Client Training 2-3 Weeks
- IT Scope Identification, Project Plan and Client Training 2-3 Weeks

Phase 2 Assessment

- Enterprise Business Controls Gap assessment 6-8 weeks
- Enterprise IT & Applications Controls Gap assessment 6-8 Weeks
- Business Controls to IT Controls Mapping 2-4 Weeks

Phase 3: Remediation

- Business Process Remediation 2-4 Weeks
- IT Process Remediation 2-4 Weeks

Phase 4: Internal Testing

- Business Internal Testing 2-4 Weeks
- IT Internal Testing 2-4 Weeks

Phase 5: Certification

- SAS 70 Compliance 2-4 Weeks
- External Auditor Testing 2-4 Weeks
- Signoff and Certification 1-2 Weeks

What are the SOX compliance project deliverables?

SOX Project Deliverables

Phase 1 Discovery

- Project Definition Document
- Project Plan With Resources and Dates, Milestone
- Executive and Managers Training Material
- Business Compliance and Reporting Templates
- IT Compliance Reporting Templates

Phase 2 Assessment

- Business Transactions Control Process Flow Diagrams
- List of mapping of all GL accounts to process flows
- List of Business Controls & Risks for each business Cycle
- IT Transactions/Process Flow Diagram
- List of IT and Applications & Risks Controls
- Mapping Biz and IT Controls (in collaboration with business managers)

Phase 3: Remediation

- Business Remediation Recommendation
- IT and Applications Remediation Recommendation

Phase 3: Testing

- Internal Testing Biz Controls Results
- Internal Testing IT Controls Results

International Institute of Management (EJ) Executive Journal

Internal Controls Best Practices

- Establish an independent internal audit function (fullt-ime) for both financial and non-financial areas (IT, operational and administrative controls and processes)
- Internal Auditors to report directly to the audit committee of the board of directors, and administratively to executive management
- Have board-approved charters for both their audit committees and internal audit departments
- Involve your external audit firm at strategic points along the SOX project timeline to ensure that they could appropriately perform internal controls attestation work for the year-end audit.
- Ensure continuous process improvement by performing enterprise/process-specific risk assessments/review once a year
- Establish project management function for the initial compliance project. The project manager role is to help establish initial project scope, structure, time , resources quality standards and processes to meet minimum SOX compliance, which normally include documentation of each process or sub-process sufficient to support a walk-through from source transactions to the financial statements, along with the identification, documentation and testing of critical controls.
- Identify significant processes and transactions outsourced to third parties. Determine their SAS 70 report will adequately support your organization's SOX financial statement assertions. Get a review and opinion of your external audit firm for its review and opinion. Include that into the project scope, time and resources
- Establish and continuously refine methodology of financial statement assertions, key control identification, documentation, testing and IT-based key controls.
- Conduct internal audit test and report on the effectiveness of the existing control activities
- Conduct management's review to correct deficiencies as noted
- Educate the management team and work in partnership with them to develop and test the effectiveness of all pertinent policies and procedures, along with evaluating the efficiency and effectiveness of the overall control environment
- Adopt COSO as the primary framework

Key Success Factors (KSF)

A successful program must be 4 dimensional

- People (Organization, Roles, Skill-sets, Training)
- Process (Business Operations; Engineering, Production, HR, IT, etc.)
- Technology (Infrastructure, Applications, Tools)
- Financial (Budget, TCO, ROI, Risk Management)

By Med Yones

IIM President