Software engineering standards for IT departments supporting Sarbanes-Oxley

.

John Walz

IEEE Computer Society, Vice President for Standards

Standards Activities Board Chair

computer.org/standards

j.walz@computer.org

IT: Information Technology

John Walz

- Sr. Consultant, The Sutton Group
  - Software / CMMI®
- Retired Lucent / AT&T
- Sr. Member IEEE, Standards Assoc.
- Chair, IEEE Computer Standards Activity Board
- Vice-Chair Planning, IEEE Software & Systems Standards Committee
- Secretary TL 9000 SIG
- Sr. Member ASQ
- Blog Author, ASQ Sarbanes-Oxley

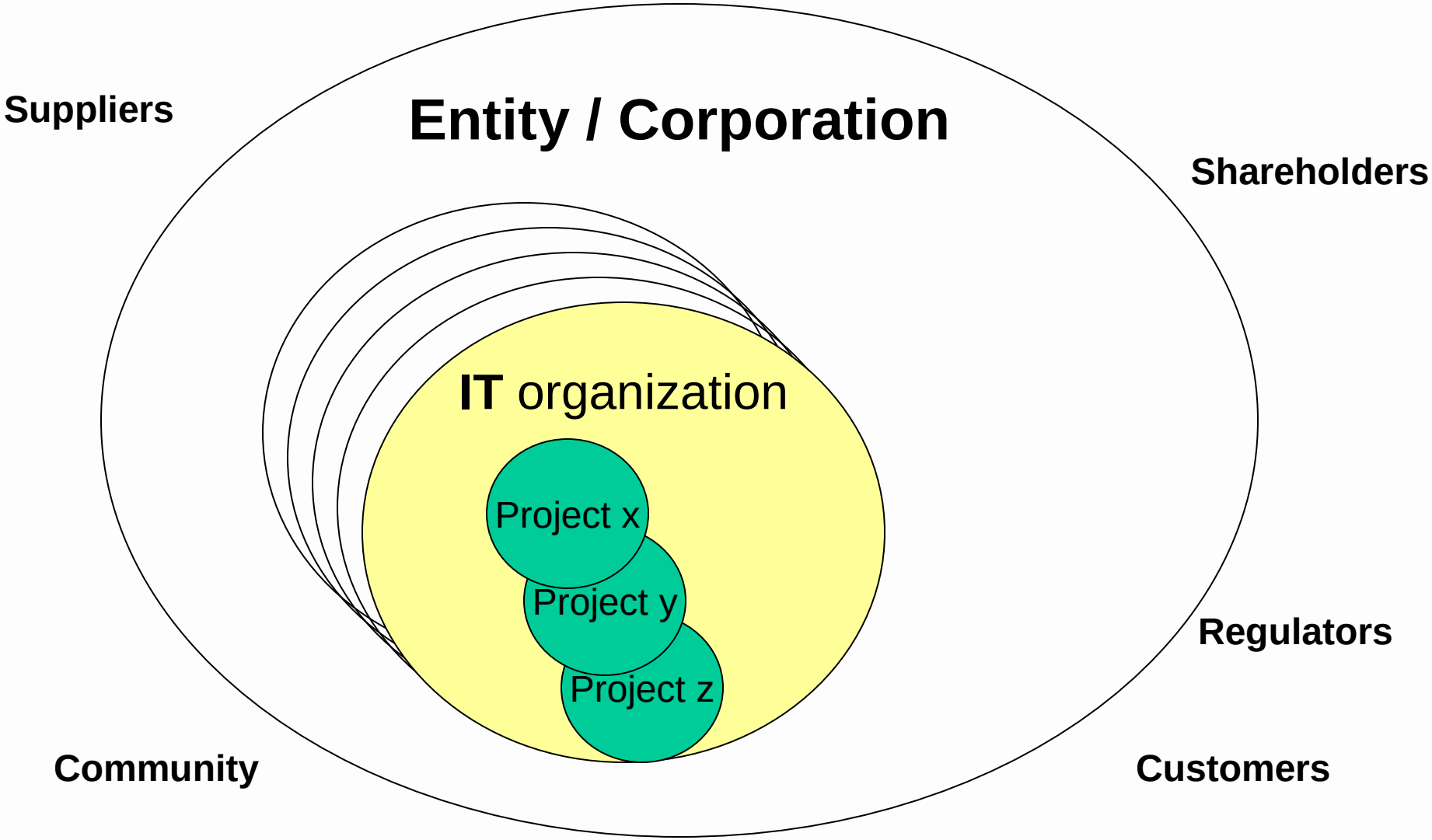
Agenda

- Risks
- Financial Regulations
- Solutions
- Frameworks & Standards
- Artifacts
- Summary

Risks by Software Engr'g Sectors

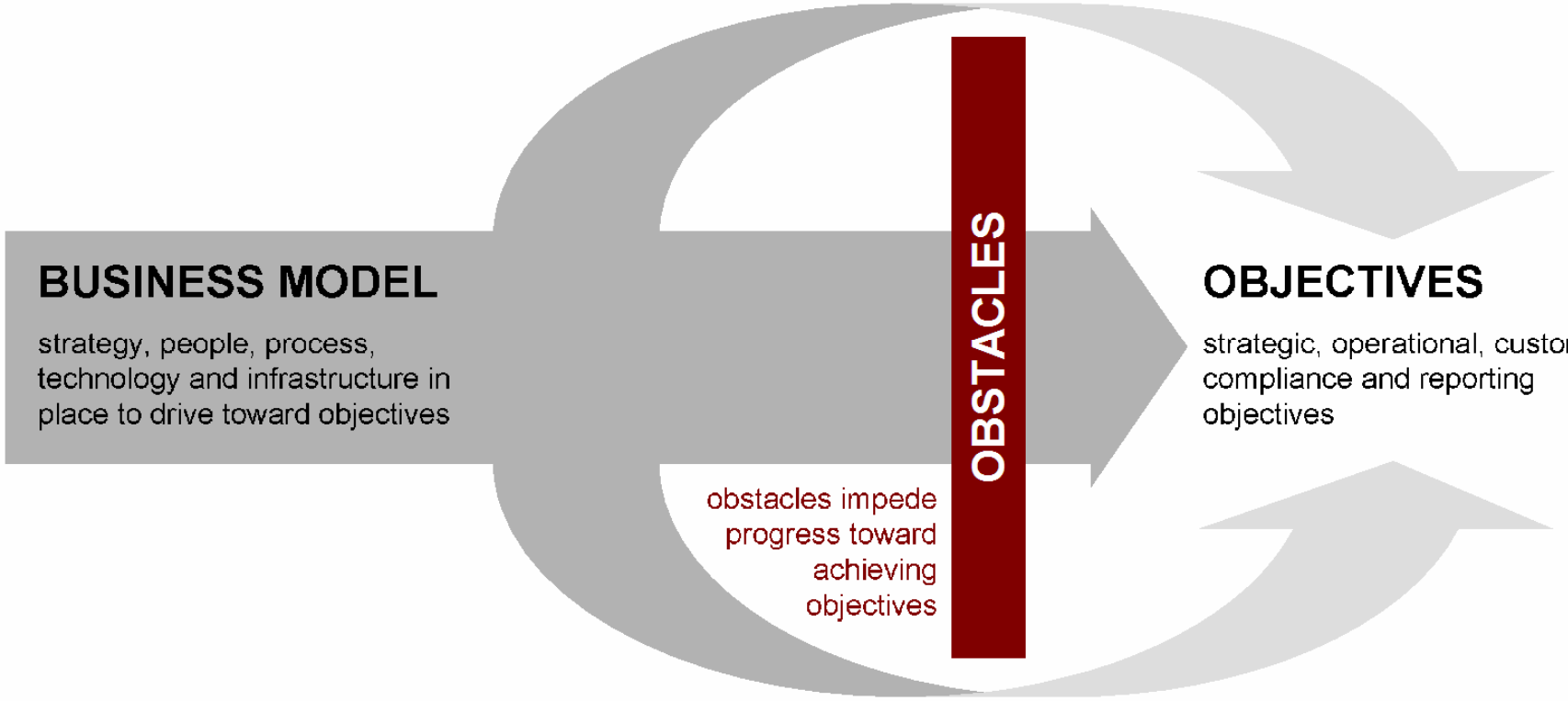
Risks Sectors:	Quality	Safety	Security	Financial
Aerospace	Hi	Hi	Med	
Military	Hi	Hi	Med	
Medical	Hi	Hi	Med	
Nuclear	Hi	Hi	Hi	
Transportation	Hi	Hi		
Biz Processes	Hi	Hi		Hi
Financial Syst.	Hi		Hi	Hi
IT Systems	Hi		Hi	Hi
Telecom	Hi	Med	Hi	
Gaming	Hi		Hi	

Entity, Organization, Project



Governance, Risk, Compliance Management

VOLUNTARY BOUNDARY — boundary defined by management including public commitments, organizational values, contractual obligations, and other voluntary policies

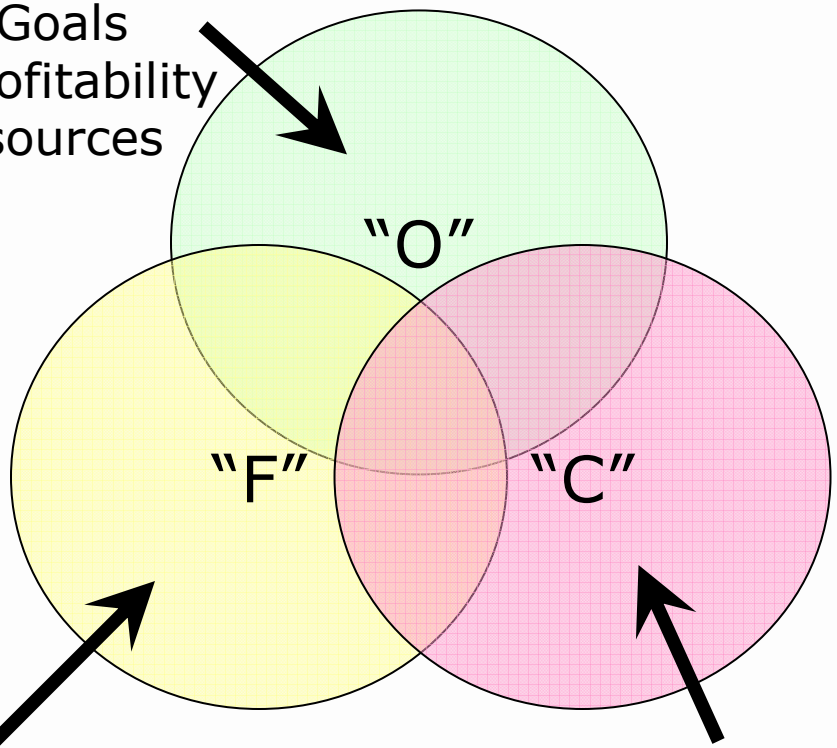


MANDATED BOUNDARY — boundary established by external forces including laws, government regulation and other mandates.

Categories of Risk (O, F, C)

O = Operational Risks Deal With Achieving Business Goals

- Performance and Profitability
- Safeguarding of Resources

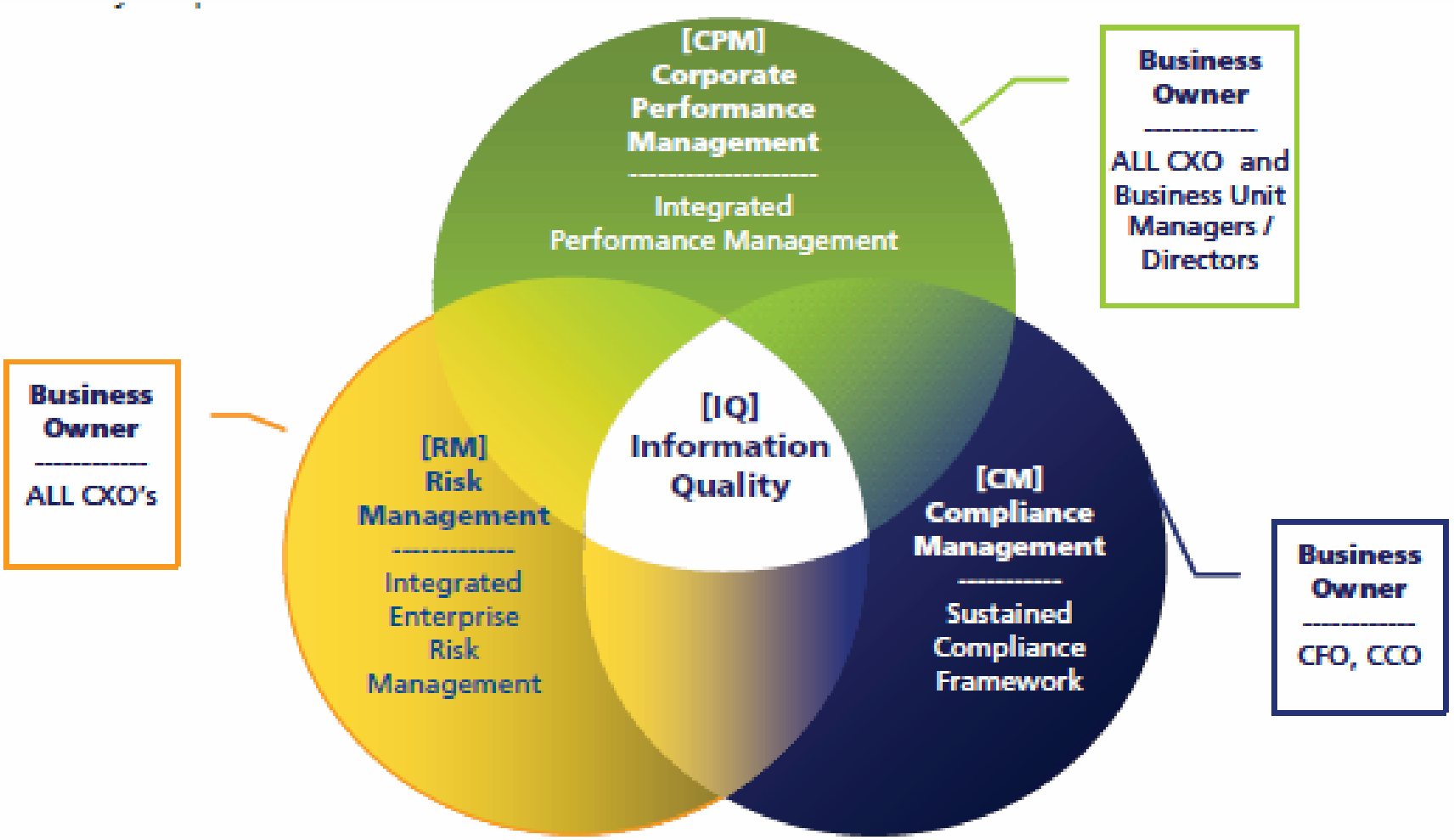


F = Preparation of Reliable Published **Financial** Statements

- Earnings Releases
- Other Public Financial Disclosures

C = Compliance with Laws and Regulations

Information Quality (IQ) Matters



GRC Issues


CURRENT STATE
In some organizations, the current state of governance, risk and compliance processes is disorganized, unnecessarily complex and fragmented
ORGANIZATIONAL & FUNCTIONAL SILOS
LACK OF VISIBILITY
POOR INTEGRATION
DUPLICATION
COMPLEXITY
ROI
HIGH COSTS
FRAGMENTATION
SLIPPING THROUGH THE CRACKS
WASTED INFORMATION
WASTED RESOURCES
VULNERABILITY
UNNECESSARY COMPLEXITY AND INFLEXIBLE

IT Organization Risks

- IT Growth → Corporation control
  - Operations, Supply Chain, Forecasting, Global, Communications, Devices, Financial
- IT Cost$ → IT outsourcing
- IT Vulnerabilities – external & internal risks
- Risk to IT commitments:
  - Quality
  - Features
  - Delivery to Customer
  - ROI to the Board of Directors (BoD)
- Governance for both Entity and IT
- Corporate governance regulations
  - Sarbanes-Oxley Act of 2002 (SOX)

Note: Entity = Corporation

Financial Risks involving IT Operations

- Information Accuracy
- Verification & Validation
- Change Control
- Corporate alignment
- Automation
- Transparency
- Separation of Duties
- Revenue Recognition
- Forecasting
- Internal Controls
- Security
- Audit trails

Top Ten IT Control Deficiencies

1. Unidentified or unresolved segregation of duties
2. Operating System access controls supporting financial applications or Portal not secure
3. Database access controls supporting financial applications not secure
4. Development staff can run business transactions in production
5. Large number of users with access to “super user” transactions
6. Former employees or consultants continue to have system access
7. Posting periods not restricted within GL application
8. Custom programs, tables and interfaces are not secured
9. Procedures for manual processes do not exist or are not followed
10. System documentation does not match actual process

* Source: Ken Vander Wal, Partner, National Quality Leader, E&Y, ISACA Sarbanes Conference , 4/6/04

IT Benefits & Risks to Internal Controls

Benefits for entity's internal control

- Consistently apply predefined business rules and perform complex calculations in processing large volumes of transactions or data.
- Enhance the timeliness, availability, and accuracy of information.
- Facilitate the additional analysis of information.
- Enhance the ability to monitor the performance of the entity's activities and its policies and procedures.
- Reduce the risk that controls will be circumvented.
- Enhance the ability to achieve effective segregation of duties by implementing security controls in applications, databases, and operating systems.

Risks to entity's internal control

- Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both.
- Unauthorized access to data that may result in destruction of data or improper changes to data, including the recording of unauthorized or nonexistent transactions or inaccurate recording of transactions.
- Unauthorized changes to data in master files.
- Unauthorized changes to systems or programs.
- Failure to make necessary changes to systems or programs.
- Inappropriate manual intervention.
- Potential loss of data.

Agenda

- Risks
- Financial Regulations
  - Mandated Boundary
- Solutions
- Frameworks & Standards
- Artifacts
- Summary

Internal Controls – U.S. history

- 1977 - Foreign Corrupt Practices Act requires Companies to establish and maintain **internal accounting controls**
- 2002 - Sarbanes-Oxley Act (SOX), Section 404(a) "each annual report that a company, " "to contain an **internal control** report: (1) stating management's responsibilities for establishing and maintaining adequate internal control structure and procedures for financial reporting; and (2) containing an assessment, as of the end of the company's most recent fiscal year, of the effectiveness of the company's **internal controls** and procedures for financial reporting."
- 2003 - SEC adopted rules implementing Section 404 with regard to management's obligations to report on **Internal Control over Financial Reporting** (ICoFR)
- 2006 - SEC proposes Section 404 guidance for management's obligations to report on ICoFR

SOX impacts for IT solutions

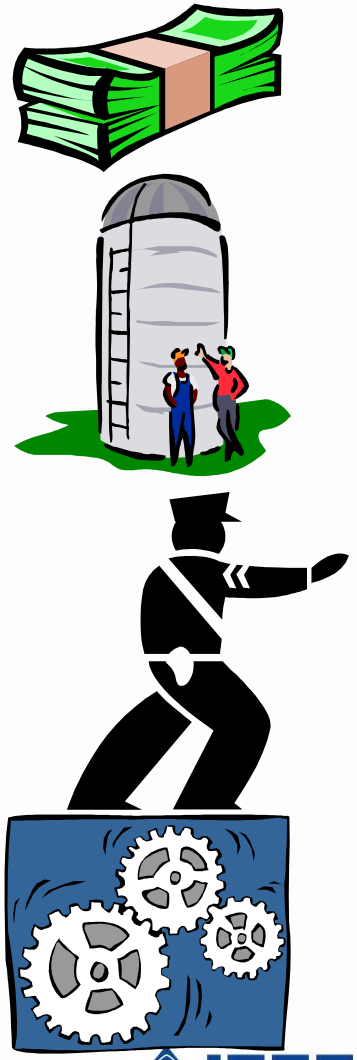
- 105: Full-time availability of data
- 301: Whistle-blowers access
- 302: Corporate responsibility for financial reports
- 403: Web site financial records
- 404: Management assessment of internal controls
- 409: Material Changes
- 802: Dealing with data
- 1102: Tampering with a record / impeding official proceeding

SOX Sections 302 & 404 - Why IT?

- **SOX Intent:** Provide top management and the Board with an accurate understanding of the financial and operational status
  - Allows Senior officers to certify material non-financial information, as well as financial information
  - IT must manage the “accurate information” for SOX compliance

IT getting involved

- High audit costs are pushing companies into more automated controls
- Disclosure requirements are driving enterprise solutions
- Internal Controls => Risk Management
  => IT Security
- Risk management is driving Continual Controls
- Transparency up to the Exec and Board and across the Process Owners required for fraud detection and whistle blowing
- Managing both manual controls and IT controls, their records, artifacts, and corrective action reports



Agenda

- Risks
- Financial Regulations
- Solutions
- Frameworks & Standards
- Artifacts
- Summary

Guidance to Management - SEC

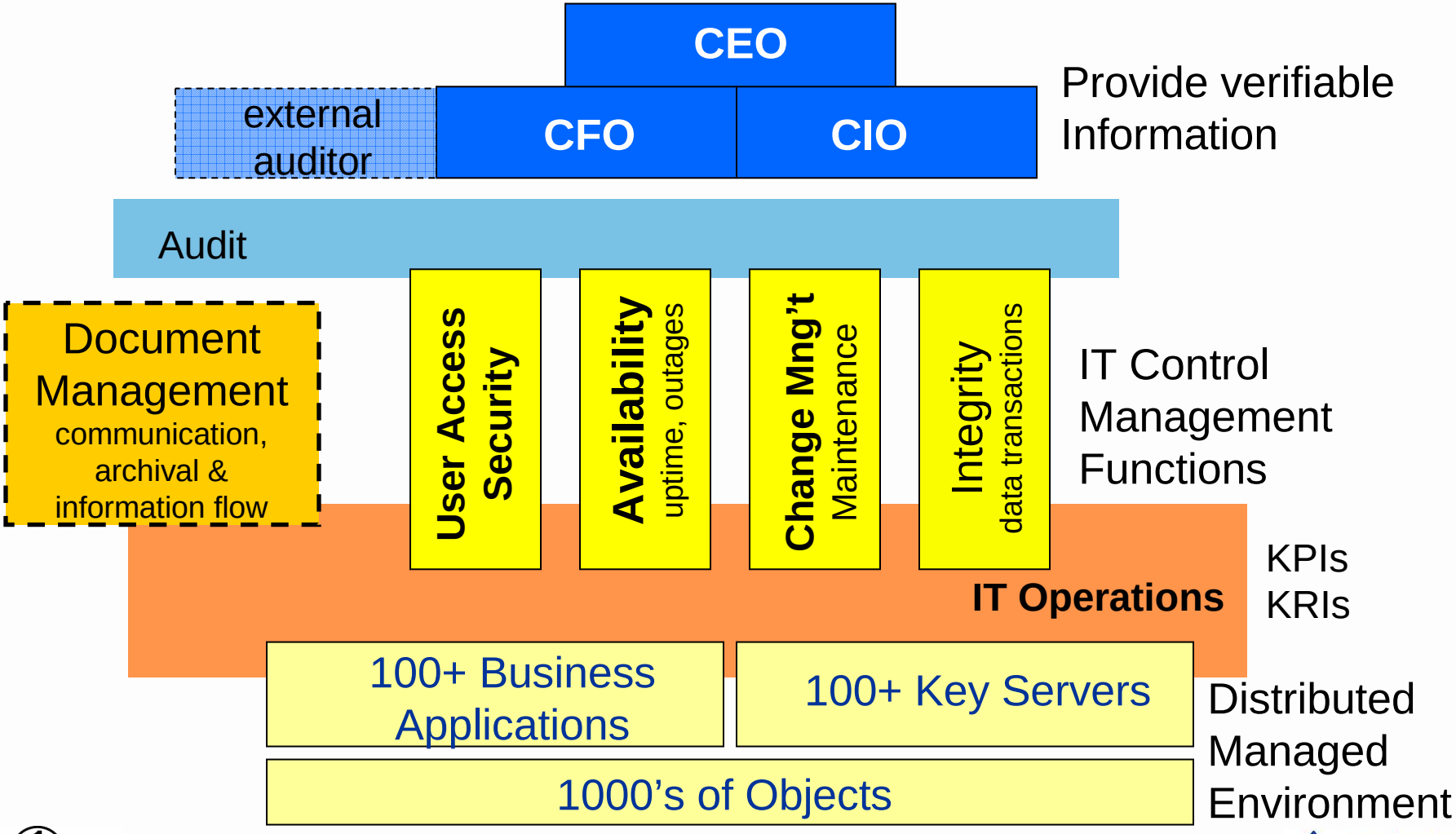
- Top-Down, Risk-based approach
- Evaluate the design of the controls
  - Identify Risks and Controls to address Risks
  - Entity-level controls
  - IT Controls (program development, program changes, computer operations, and access to programs and data)
- Evaluate evidence about the operation of its controls
  - self-assessments, in low-risk areas and perform more extensive testing in high-risk areas
- Key Principles
- Reporting
  - Internal Control Deficiencies
  - Material Weaknesses Disclosures
  - Restatement of Financial Statements

SOX 302 & 404 compliance - Strategic priorities

- Improving IT management and governance to enhance controls and relevance to the business
- Focus on:
  - enhancing management processes and controls,
  - refining systems architecture, and
  - aligning IT with business needs

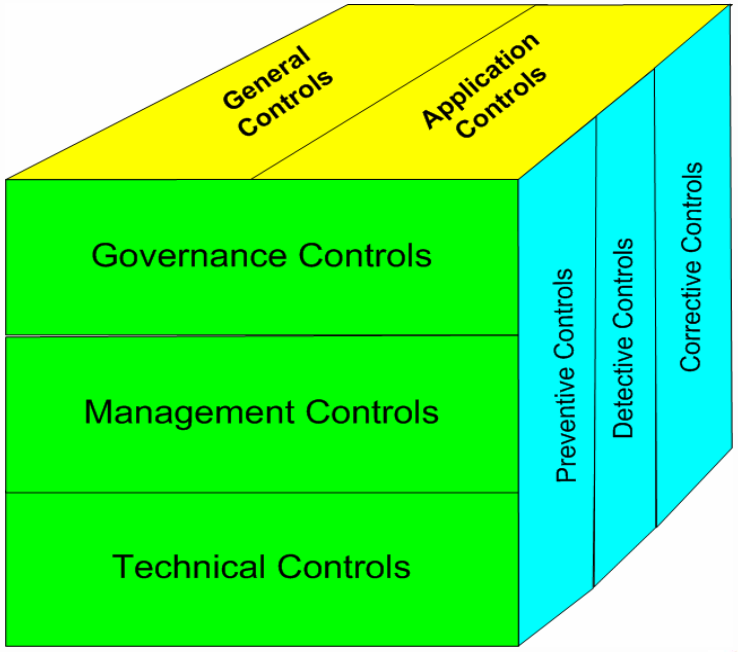
Challenge

monitoring risk and management response



Understanding IT Controls

- IT control is a process that provide assurance for information and information services, and help to mitigate risks associated with use of technology.
- Two components
  - Automation of business controls
  - Control of IT
- An IT control classification



IT Key Control Objectives

1. Maintain a complete secure **versioning** & audit history of software, process, policy, and processes change.
2. Develop a **formal systems development methodology**.
3. Implement **requirements management** with user and IT approvals.
4. Ensure maintenance and versioning of project documentation.
5. Define **systems requirements**.
6. Develop a system acquisition and change approach addressing security risks and data conversion.
7. Ensure separation of development and production activities.
8. Model and automate processes.
9. Engage in **rigorous testing** including use cases.
10. Control movement of applications by development personnel from test to production.
11. Automate approval process ensuring management review and approval of IT solutions prior to implementation.
12. Construct an implementation review process for system modifications made in an emergency.
13. Enforce formal policies and procedures defining system security.
14. Ensure user account security parameters are in place and enforced.

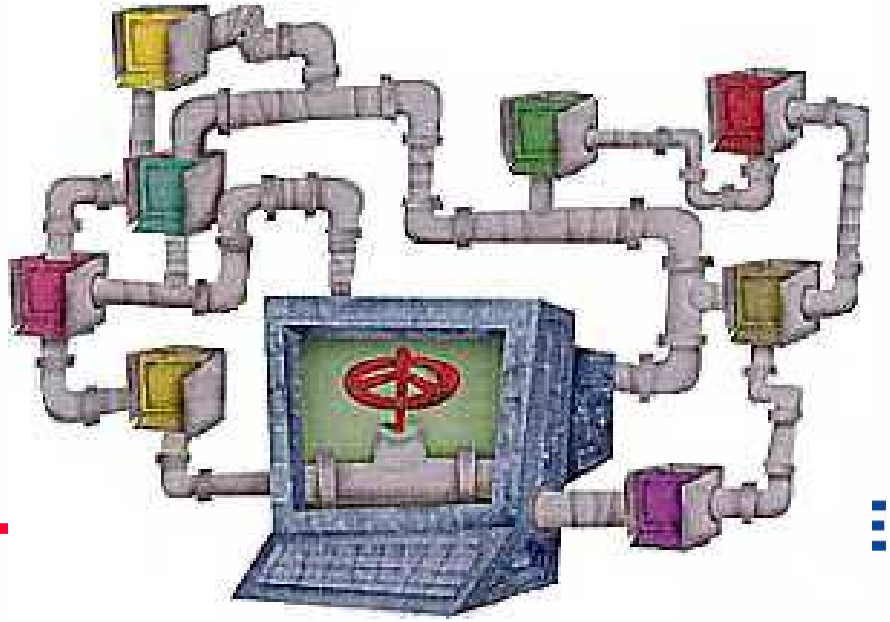
MKS Enterprise Change Management Solution and Six-Step Delivery Model for Sarbanes-Oxley Compliance Readiness
Dietrich, 2006

Qualitative characteristics of financial and business information

- Relevance
  - Timeliness
  - Predictive value
  - Validation of expectations
- Reliability
  - Measurability
  - Completeness
- Neutrality
  - Unbiased
- Comparability
  - Industry peers
  - Period-to-period
- Understandability
  - Clear
  - Coherent
  - Jargon-free

Types of SOX Support Software & SOX Enterprise Solutions

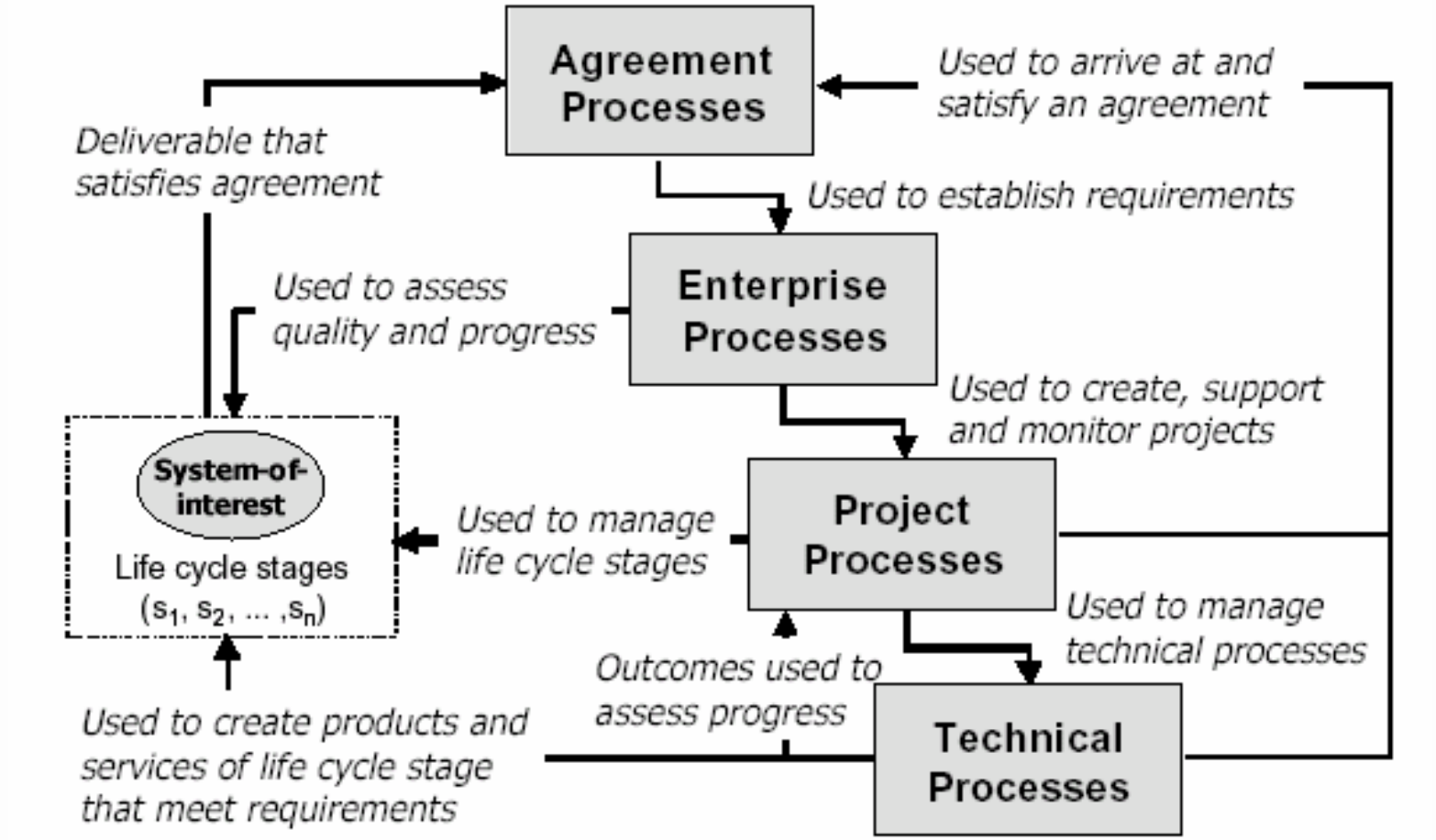
- Risk and Control Management
  - Flowcharting tools
  - Risk databases
  - Employee survey software
- Audit Management
- Data Analysis
  - Querying,
  - Data mining,
  - Financial statement examination tools
- Employee Training
- Section Compliance
- Enterprise Content Management
- Enterprise Portfolio Management
- Enterprise Project Management
- Corporate Authorization Management



Design your organization

- Most laws assume or imply the need for proper implementation
- Regulations are by design prescriptive, rather than descriptive
- Excellent IT processes are required to support SOX compliance for accuracy and resistance to errors and fraud
- Process definition is hard work
- Governance of IT Processes is critical

Process Categories

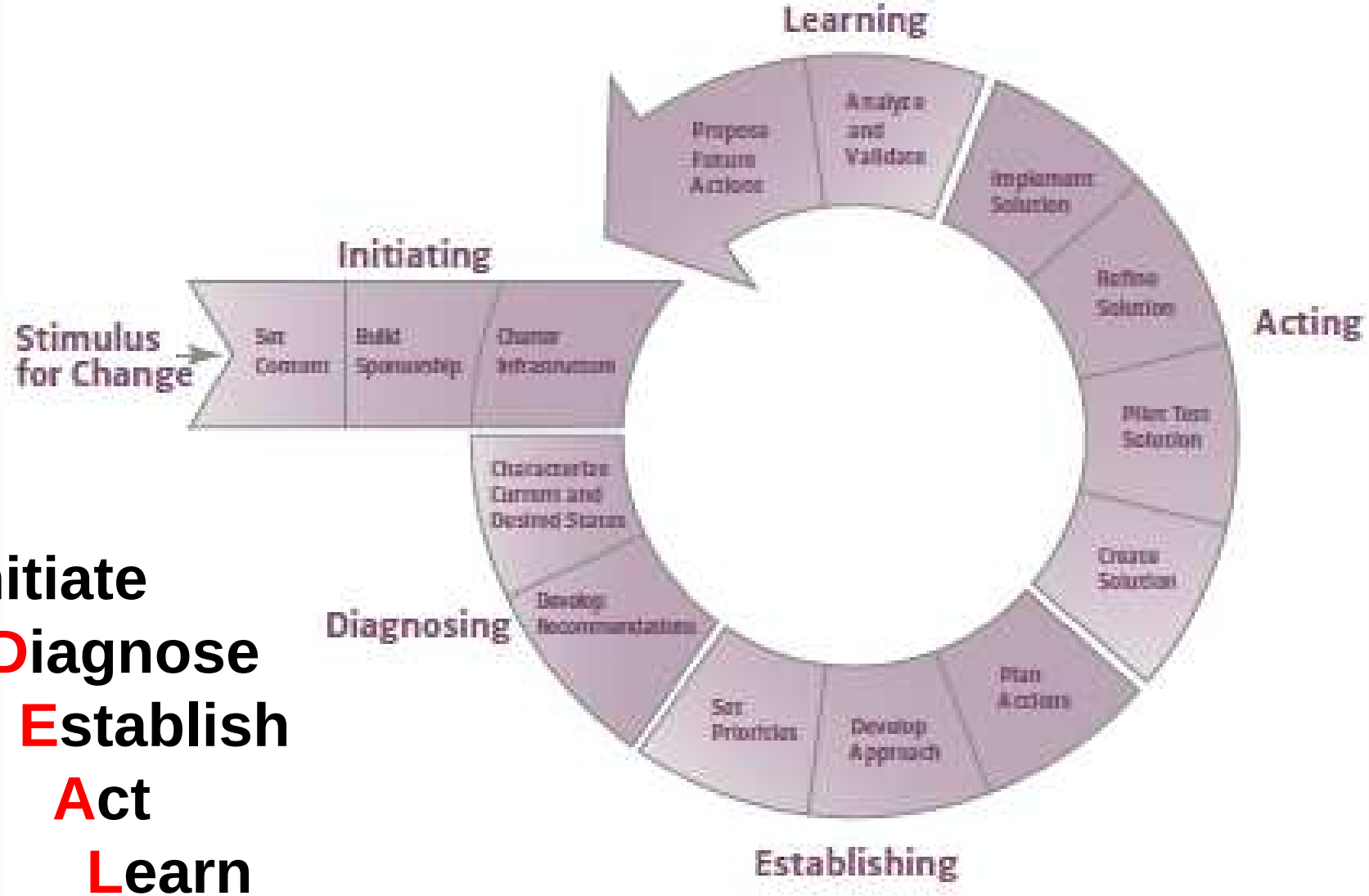


IT documents and records (artifacts)

- **Documents and records provide:**
  - **Communications within the team and to stakeholders**
  - **Foundation for improvement**
  - **Evidence of compliance**

- **IT organizations**
  - **Can chose from several frameworks, standards, and methods to implement and enhance their mission and value-added services within their company**
  - **Have freedom on the format and content of typical software engineering project documents**

IDEAL^{SM} Improvement Model - SEI



Initiate
Diagnose
Establish
Act
Learn

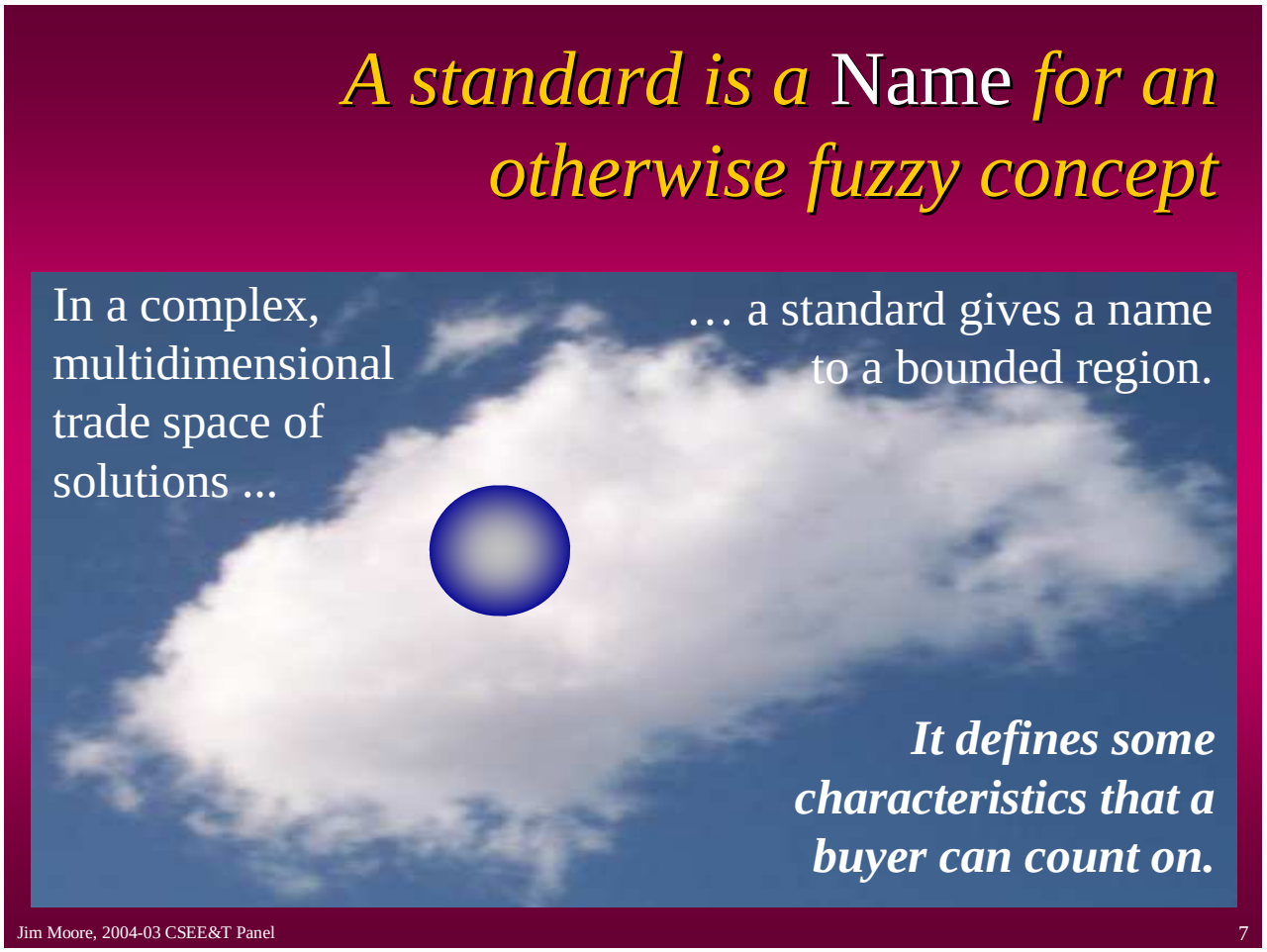
Recommendations for IT support of SOX Objectives

- Provide continuous, accurate information to top executives and the Board of Directors
- Value Added approach beyond Compliance for Governance and Risk Management
- Make Investments in sustainability, long-term infrastructure
- Design IT to meet the Spirit and Intent of SOX for your business objectives
- Design IT into your Enterprise
- Design enterprise IT solutions with effective automated controls
- Implement Continuous Controls
- Process Management approach

Agenda

- Risks
- Financial Regulations
- Solutions
- Frameworks & Standards
- Artifacts
- Summary

Value of Standards



- What is "testing"?
- Sftw Engr needs standards to assign names to practices or collections of practices.
- This enables communication between Buyer and Seller
- Standards represent the "minimum level of responsible practice"

Frameworks & Standards

- Frameworks and Standards are used for
  - 1) strategic governance initiatives, or
  - 2) to meet regulatory and audit compliance
- Standards Areas:
  - Management
  - IT operations
  - IT development - Software Engineering

Frameworks and Standards for IT

- Management
  - International Organization for Standards – ISO 9001 Quality Management System
  - COSO – Internal Controls, Enterprise risk management
- IT operations
  - IT Governance Institute - Control Objectives for Information & Related Technology (CobiT)
  - UK - IT Infrastructure Library (ITIL) for Service Management
  - ISO 20000 IT Service Management
  - ISO 27000 Info. Security Management System
- IT development - Software Engineering
  - SEI - Capability Maturity Model (CMMI-Dev)
  - IEEE software engineering standards

IEEE Standards

IEEE

- **IEEE Standards Association**
  - **→ American National Standards**
  - **→ ISO and IEC and JTC1**
- **IEEE Computer Society**
  - **Standards Activities Board** computer.org/standards
    - VP for Standards, Sponsor Chairs (12), Liaisons (9), Committee Chairs (4)
  - **Standards Committee Sponsors**
    - Working Groups, multiple / Sponsor
      - **Over 5,000 Volunteers, some are CS members**
      - **Working over 700 standards**
      - **Create draft standards for balloting**
    - Balloting Groups
      - **Broad group of IEEE-SA members who vote and comment on draft standards**

What are IEEE Software Engr. Standards?

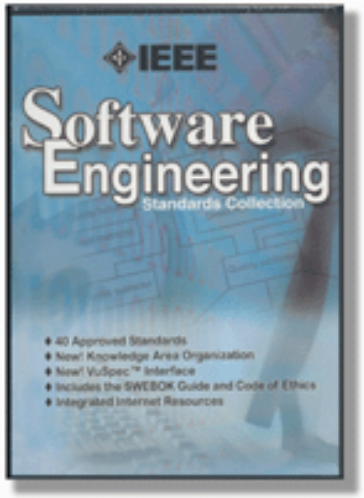
- **Represent** industry best practices
  - **Codifies industries best practices for all critical software engineering processes and their outputs**
  - **Developed by domain experts with broad expert consensus.**
- Specify content
  - **Provide** detailed procedure explanations **and offer section by section** guidance **on building the necessary documentation**
  - **with no recommendation of exact techniques or formats**
  - **Used as tools to help in the painful process of** 'self-documentation'
- **Specify the minimum required contents for each** support document or artifact

Software Engineering Standards for IT Development

- IEEE/ISO/IEC 12207, Software Life Cycle Processes
  - Describes 17 processes spanning the life cycle of a software product or service
  - The standard is somewhat prescriptive in defining a minimum level of responsible practice
- IEEE/ISO/IEC 90003, Application of ISO 9001 to Computer Software
- 40 other IEEE standards

IEEE Software Engineering Standards Collection

- **Over 40 of the most current IEEE software engineering standards on CD-ROM**

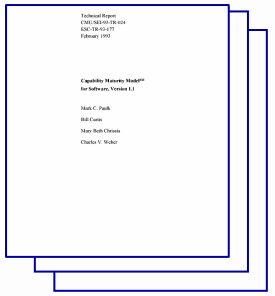


ISBN 0-7381-3757-X, Sep03, Catalog # ST01121, $370.00 Members / $465.00 List

Agenda

- Risks
- Financial Regulations
- Solutions
- Frameworks & Standards
- Artifacts
- Summary

Work Product / Artifact



Definitions from CMMI®

- Work Product is any artifact produced by a process.
- Artifacts can include files, documents, parts of the product, services, processes, specifications, and invoices.
- A key distinction between a work product and a product component is that a work product need not be engineered or part of the end product

Minimum IT Documentation

- Information Security
  - Policies, Procedures, Standards
  - Risk Assessment
  - Authentication Controls
  - Authorization Controls (including Administrator/Super User level)
  - User Access Administration (Granting, Terminating and Employee Transfers, Contractors)
  - Security Logging and Monitoring Controls
  - Other Technical Configurations
  - Physical Security
- Relevant application controls (e.g., Access Controls, Edit/Validation Checks, Interfaces, Audit Trails, etc.)
- Systems Development and Change Management Controls
  - Request/Approvals
  - Prioritizations
  - Development Standards
  - Sftw Dev Life Cycle
  - Testing, QA, Migration
  - Documentation Maintenance
- Computer Operations
  - Batch Jobs (Abends, Performance/Capacity Monitoring)
  - Backups

Requirements Management Artifact

- Software Requirements Management Plan

IEEE Standard 830, Practice for Software Requirements Specifications.

Outlines the requirements for what comprises a good Software Requirements Specification (SRS):

- Establishes basis for agreement between customers and suppliers on what the software product is to do
- Reduces the development effort
- Provides a basis for estimating costs and schedules
- Provides a baseline for validation and verification
- Facilitates transfer
- Serves as a basis for enhancement

Requirements Management Artifact

- Software Requirements Management Plan document outline

Table of Contents
Revision Sheet
1.0 Introduction
2.0 Purpose
  2.1 Scope
  2.2 Definitions
  2.3 Goals
3.0 References
  3.1 Key Acronyms
  3.2 Key Terms
  3.3 Key References
4.0 Management
  4.1 Organization
  4.2 Tasks
  4.3 Responsibilities
    4.3.1 Management
    4.3.2 Program Manager
    4.3.3 Project Lead
    4.3.4 Team Members
    4.3.5 Customer
5.0 Software Requirements Management Overview
  5.1 Software Requirements Modeling Techniques
    5.1.1 Functional Analysis
    5.1.2 Object-Oriented Analysis
    5.1.3 Dynamic Analysis
  5.2 Software Requirements Management Process
    5.2.1 Requirements Elicitation
    5.2.2 Requirements Analysis
    5.2.3 Requirements Specification
  5.3 Characteristics of a Good SRS
    5.3.1 Correct
    5.3.2 Nonambiguous
    5.3.3 Complete
    5.3.4 Verifiable
    5.3.5 Consistent
    5.3.6 Modifiable
    5.3.7 Traceable
    5.3.8 Usable During Operation and Maintenance
6.0 Standards and Practices
7.0 Software Measurement and Metrics
8.0 Verification and Validation
9.0 Software Configuration Management
10.0 Developing a Software Requirements Specification

Appendix A // Project Software Requirements Specification Template
Appendix B// Requirements Traceability Matrix

Practical Support for CMMI®-SW Project Documentation: Using IEEE Software Engineering Standards

www.wiley.com/WileyCDA/WileyTitle/productCd-0471738492.html

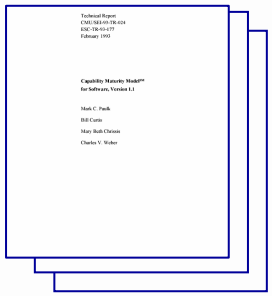
IEEE COMPUTER SOCIETY

Agenda

- Risks
- Financial Regulations
- Solutions
- Frameworks & Standards
- Summary

Recommendations for IT development to support SOX Objectives

- Process Management approach, aligned to your business objectives and standards
- Build IT into company's Management System (ISO 9001)
- Use ISO 20000 or ITIL for generic IT processes
- Use CobiT to defined IT operational processes with important security requirements
- Use CobiT & ISO 27000 for extensive security requirements
- Use IEEE Software Engineering standards to define IT development processes and artifacts
- IT development and operations artifacts
  - Stored in Configuration Mgmt System
  - Used by continuous controls, process owners, internal and external financial audits



Questions?