Sarbanes-Oxley Act and QA
A Marriage of Convenience

Presented by
"Dr. Rebecca" Staton-Reinstein
Ph.D., CSQA

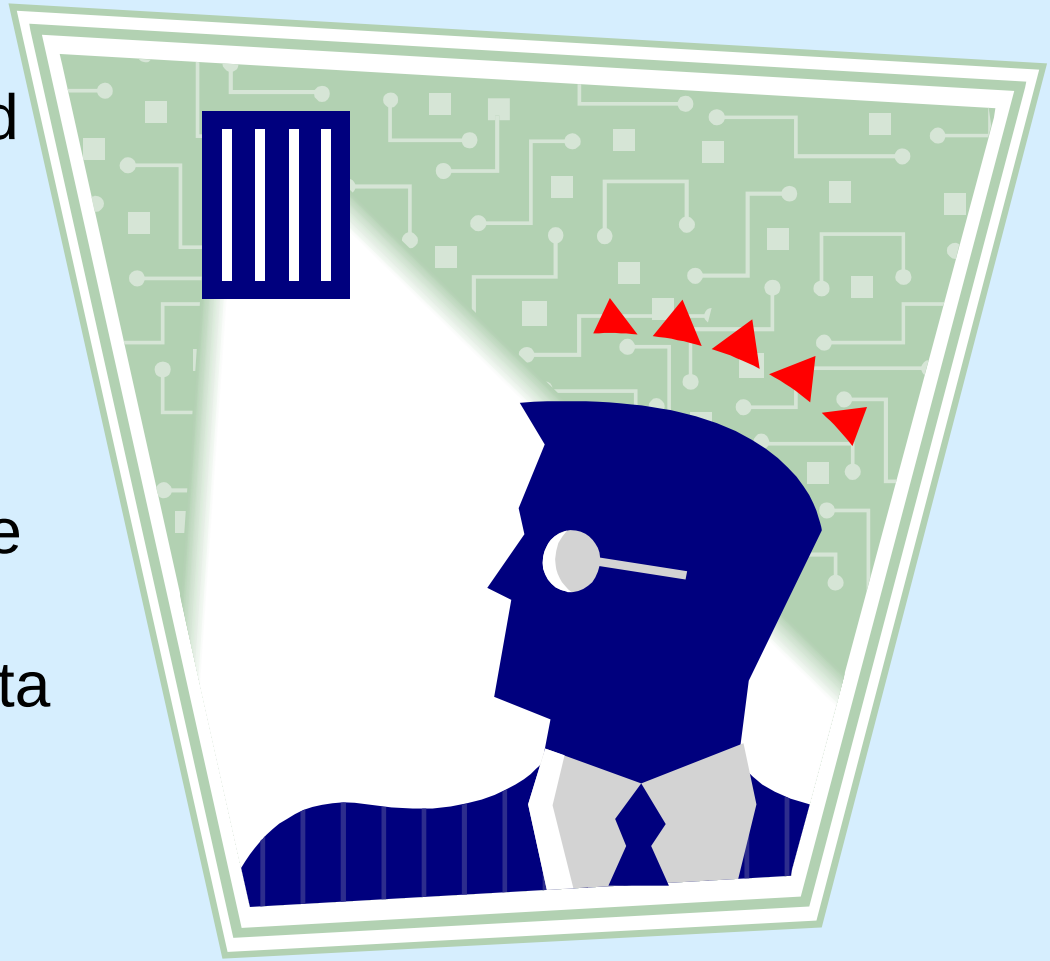
The significant problems we face cannot be solved at the same level of thinking we were at when we created them.

- Albert Einstein

Albert Einstein seeks inspiration, California, 1933.

What is Sarbanes-Oxley

- US Legislation focused on fraud
- Initiated after several corporate scandals, beginning with Enron
- Holds CEO, CFO liable for accuracy, integrity, security of financial data
- Heavy penalties, including jail, for non-compliance



Sarbanes-Oxley Act = SOX

- Initially applied to all companies regulated by SEC – US Securities & Exchange Commission; US and non-US-based
- Voluntarily adopted by some DOD, other government departments
- Major accounting firms requiring other large clients to adopt for uniformity of external audit procedures

Why should we care?

- CEOs holding CIOs fully accountable for accuracy, integrity, security of data
- Audits focus on key IT/software processes that affect data
- Many of these processes fundamental to assuring software quality

SOX TRUMPS EVERYTHING

- Integrity of data and systems
- Security of data and systems
- Processes **defined and used**
- Independent audits

SOX section 404: must address these objectives:

- Access Control -- monitor attempts to access the company's financial reporting system or the data that feeds the system.
- Configuration Control -- monitor the configuration, policies and software installed on systems covered by SOX & systems with access to that system.
- Malicious Software Detection -- collect . report malicious activities caused by viruses, other malicious code with centralized analysis.
- Policy Enforcement -- verify all users are complying with regulations to reduce the chance of accidental exposure of sensitive information.
- User Monitoring and Management -- create complete audit of non-employee private data activities; minimize risk from compromised accounts.
- Environment & Transmission Security -- monitor environment to ensure that security threats are detected, corrected quickly through proactive measures; ensure that the transmission of sensitive data is secured and done with the proper encryption levels.

Sarbanes-Oxley Act (SOX)

- Requires Officers, Board certify accuracy, security, integrity of corporate financial data and systems that "touch" those data
- Requires Risk Control Process for S/W Processes:
  - SDLC Process ☑
  - Functional Specification ☑
  - Detail Design Specification ☑
  - Unit Testing ☑
  - User Acceptance Testing ☑
  - Configuration Management ☑

Systems Development Life Cycle

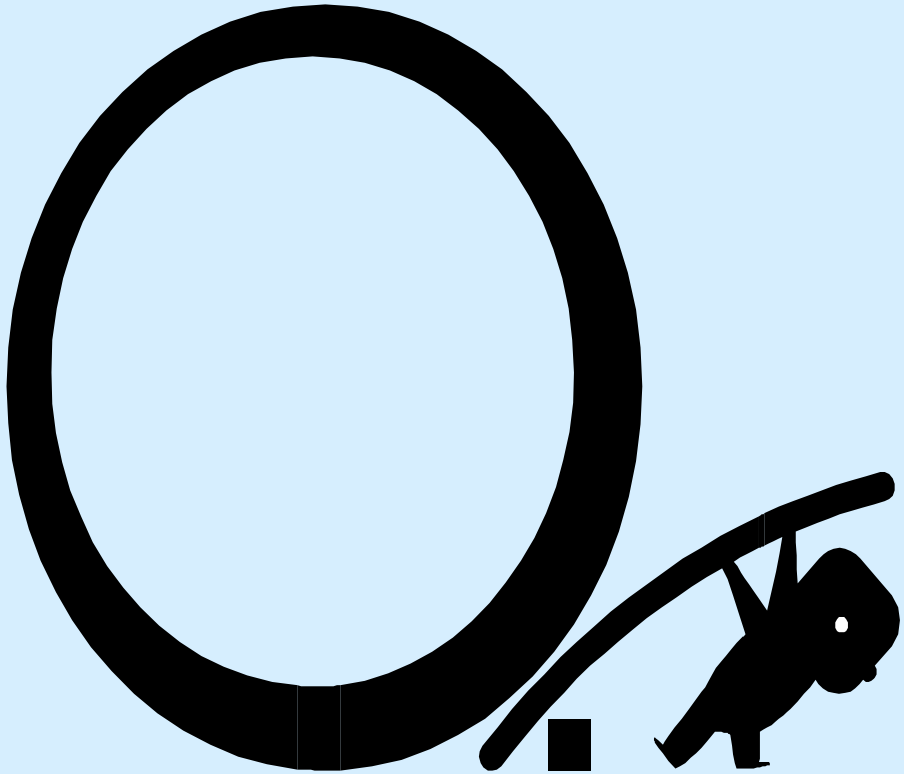
SOX Risk Control	*Typical Templates*
SDLC Process ☑	SDLC + Responsibilities
Functional Spec ☑	Requirements Specification
Detail Design Specification ☑ {	Preliminary Design Spec Detail Design Spec
Unit Testing ☑ {	Unit Test Plan Integration Test Plan
System Testing ☑	System Test Plan
UAT ☑	User Acceptance Test Plan

Additional Components Supporting Intent of SOX

Documents
Quality Assurance Implementation Plan
Project Quality Assurance Plan
System Review Standards and Procedures
Test Tool Standardized User Manual

Using SOX as leverage

- Familiarize yourself with SOX requirements
- Map SOX requirements to existing processes, SDLC, standards, other IT/ Software quality initiatives
- Demonstrate relationships
- Demonstrate ROI



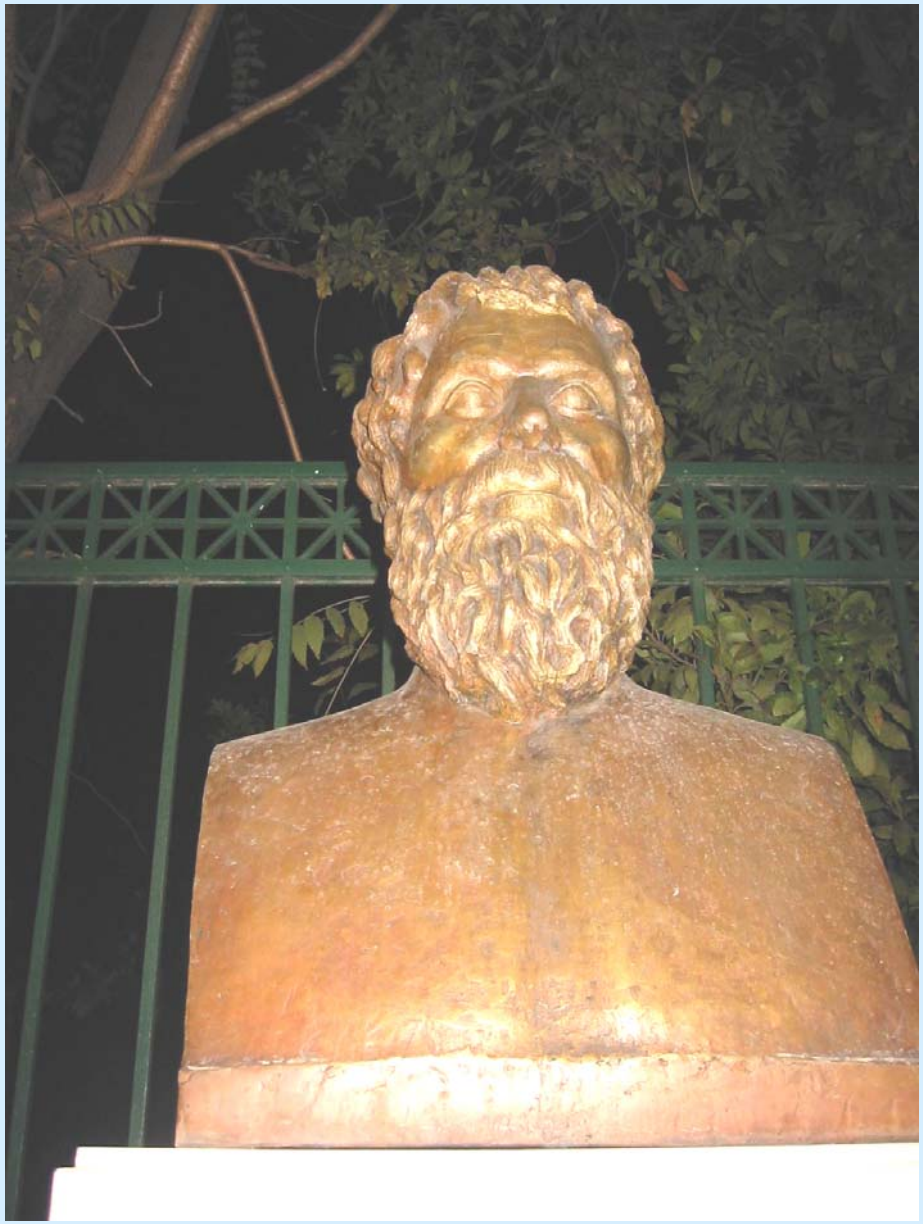
SOX Relation to Quality

- Quality Assurance = Prevention Processes
- Quality Control = Find Defects/Test/Review
- Quality Improvement = Reduce Defects, Variation in Process, Product
- SOX = Defined Processes/Used
- SOX = Internal, External Audits
- SOX = Use Audit Findings to Improve Processes

References

References available at presentation

Or by request at
DoctorRebeccaSR@cs.com



Knowledge must come through Action

-- Sophocles