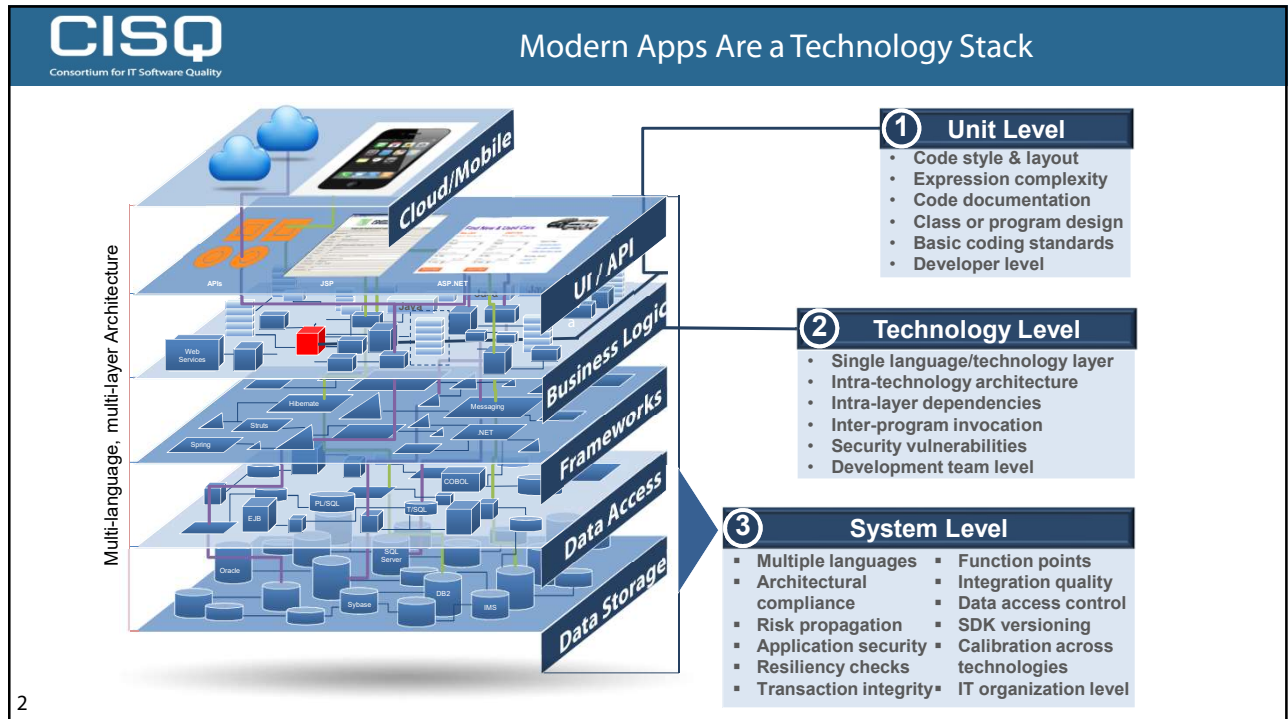
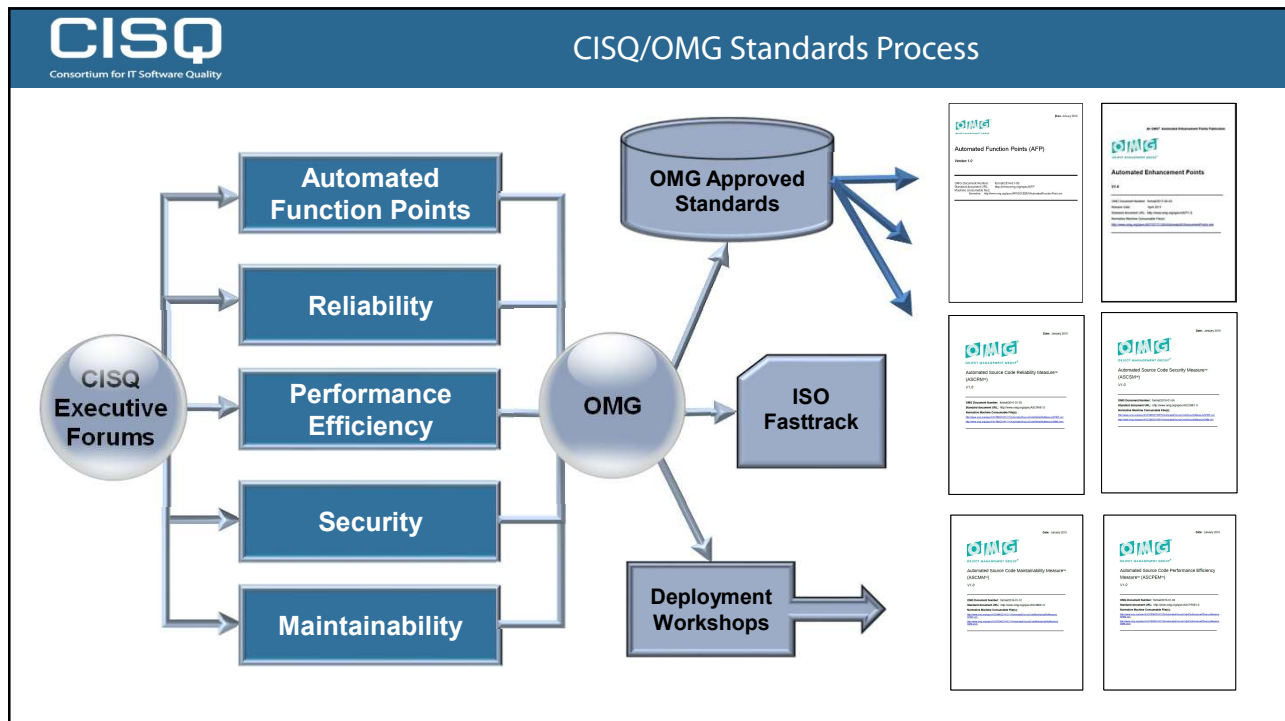
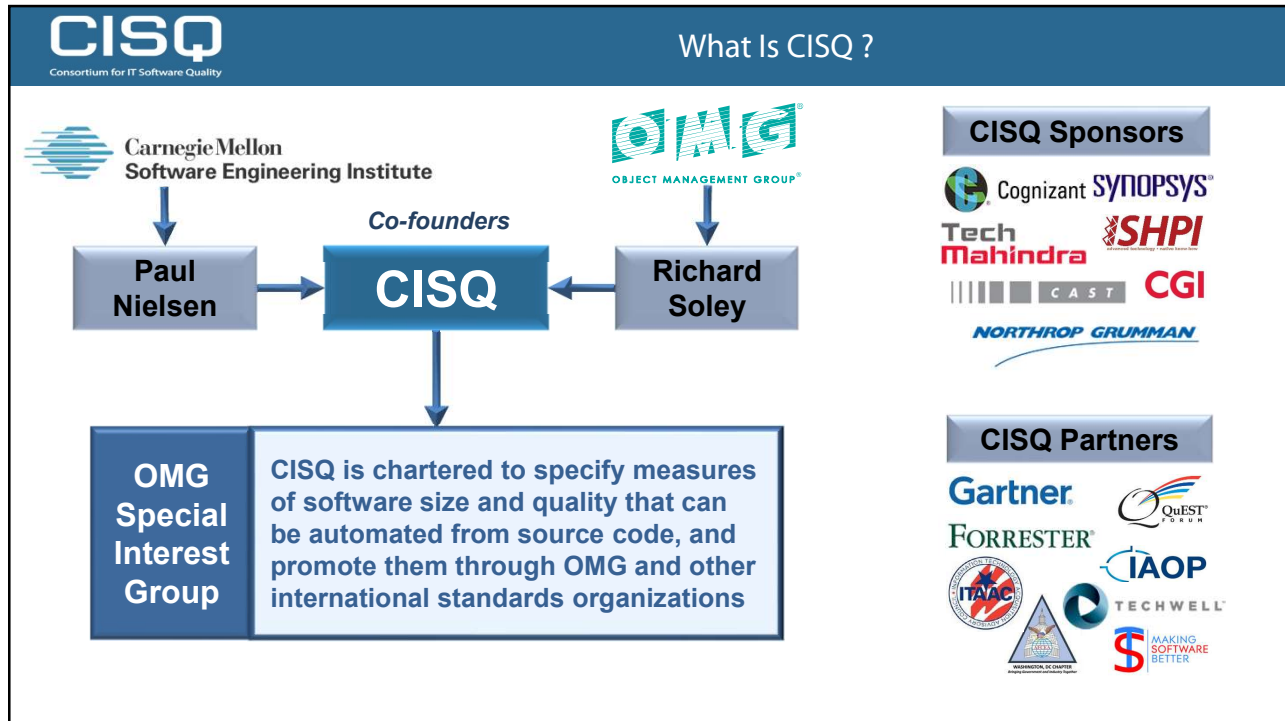


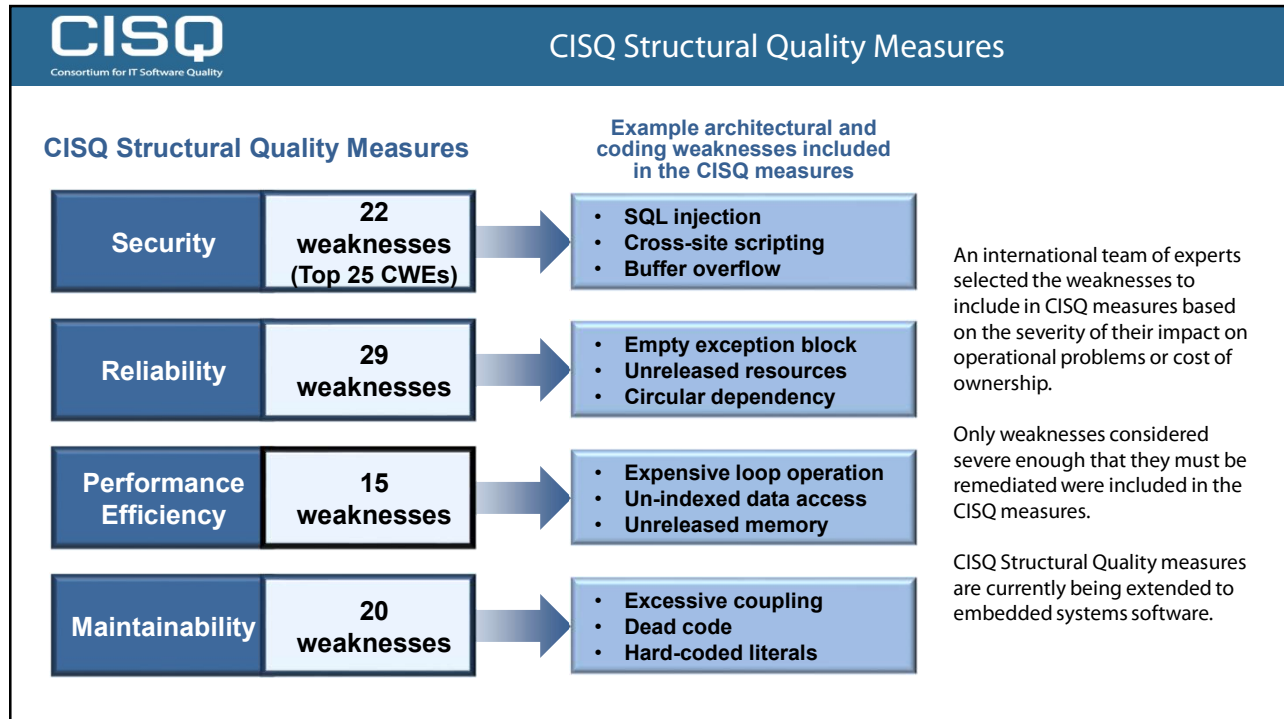
Advances in Measuring Software Quality and Technical Debt

Dr. Bill Curtis
Executive Director, CISQ

CISQ International Standards for Automating Software Size and Structural Quality Measurement
Consortium for IT Software Quality









CISQ
Consortium for IT Software Quality

22 (of Top 25) CWEs Form the CISQ Security Measure

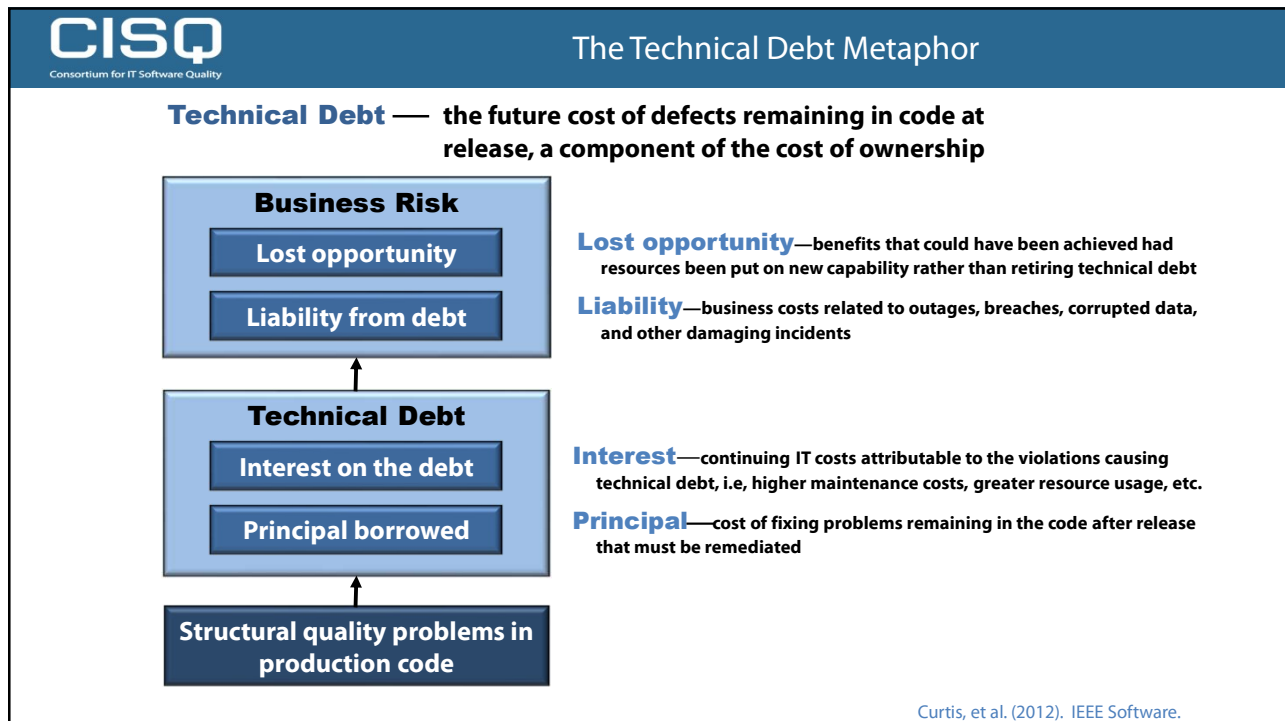
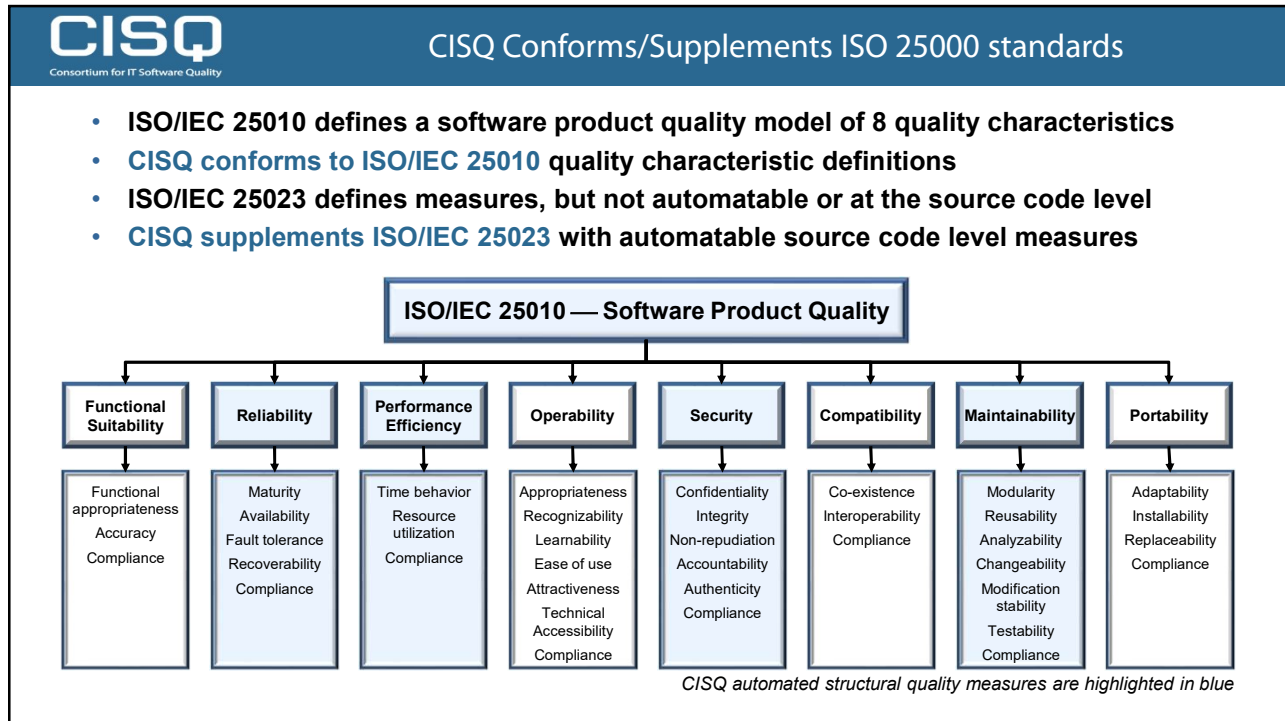
- **CWE-22** Path Traversal Improper Input Neutralization
- **CWE-78** OS Command Injection Improper Input Neutralization
- **CWE-79** Cross-site Scripting Improper Input Neutralization
- **CWE-89** SQL Injection Improper Input Neutralization
- **CWE-120** Buffer Copy without Checking Size of Input
- **CWE-129** Array Index Improper Input Neutralization
- **CWE-134** Format String Improper Input Neutralization
- **CWE-252** Unchecked Return Parameter of Control Element Accessing Resource
- **CWE-327** Broken or Risky Cryptographic Algorithm Usage
- **CWE-396** Declaration of Catch for Generic Exception
- **CWE-397** Declaration of Throws for Generic Exception
- **CWE-434** File Upload Improper Input Neutralization
- **CWE-456** Storable and Member Data Element Missing Initialization
- **CWE-606** Unchecked Input for Loop Condition
- **CWE-667** Shared Resource Improper Locking
- **CWE-672** Expired or Released Resource Usage
- **CWE-681** Numeric Types Incorrect Conversion
- **CWE-706** Name or Reference Resolution Improper Input Neutralization
- **CWE-772** Missing Release of Resource after Effective Lifetime
- **CWE-789** Uncontrolled Memory Allocation
- **CWE-798** Hard-Coded Credentials Usage for Remote Authentication
- **CWE-835** Loop with Unreachable Exit Condition ('Infinite Loop')

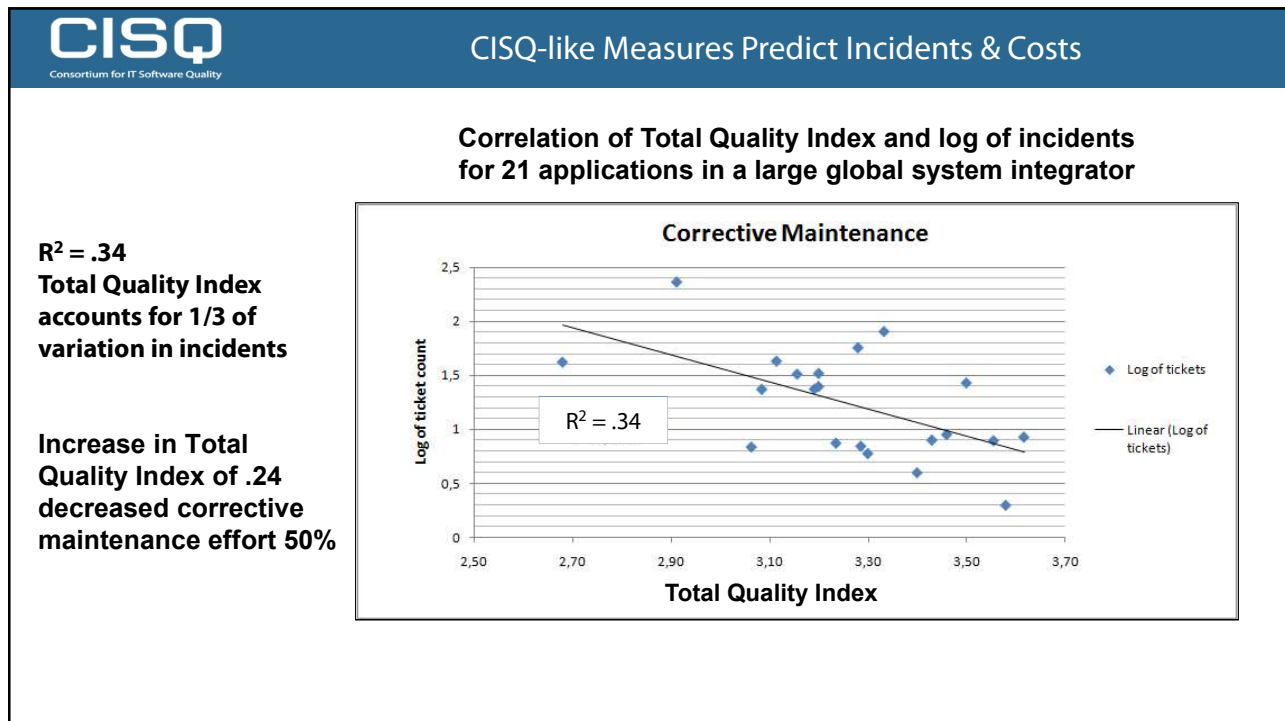
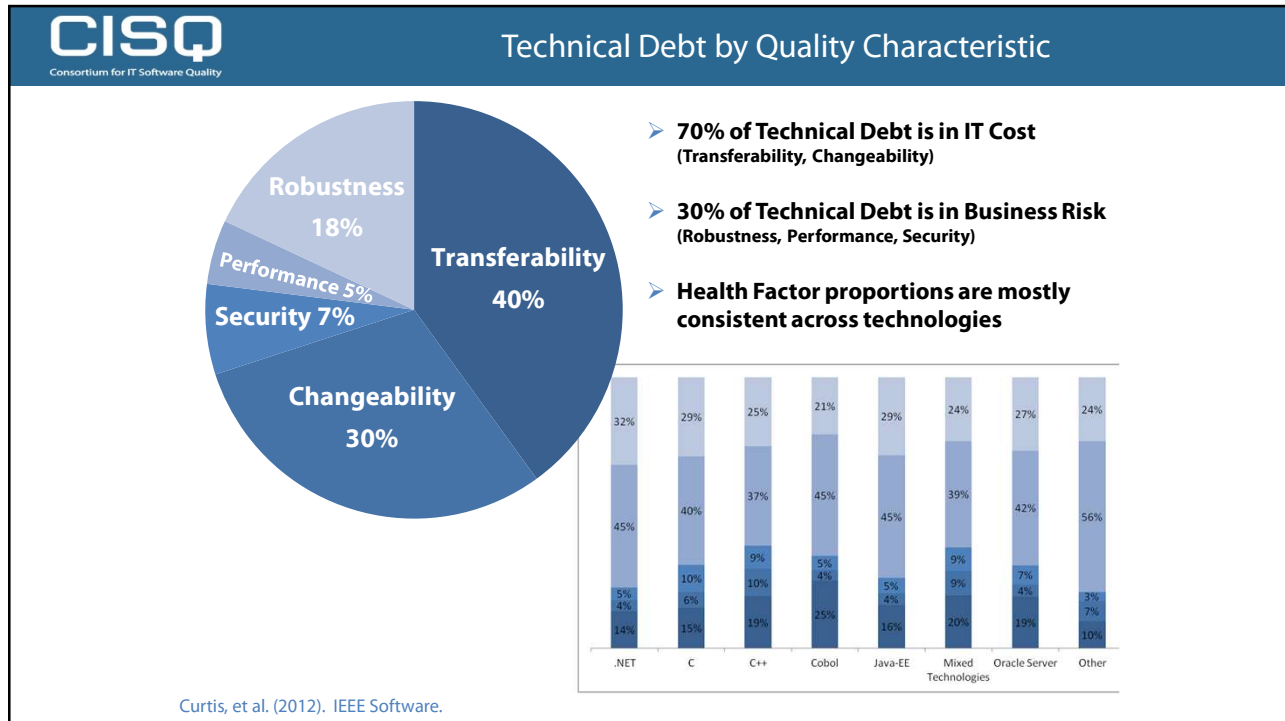


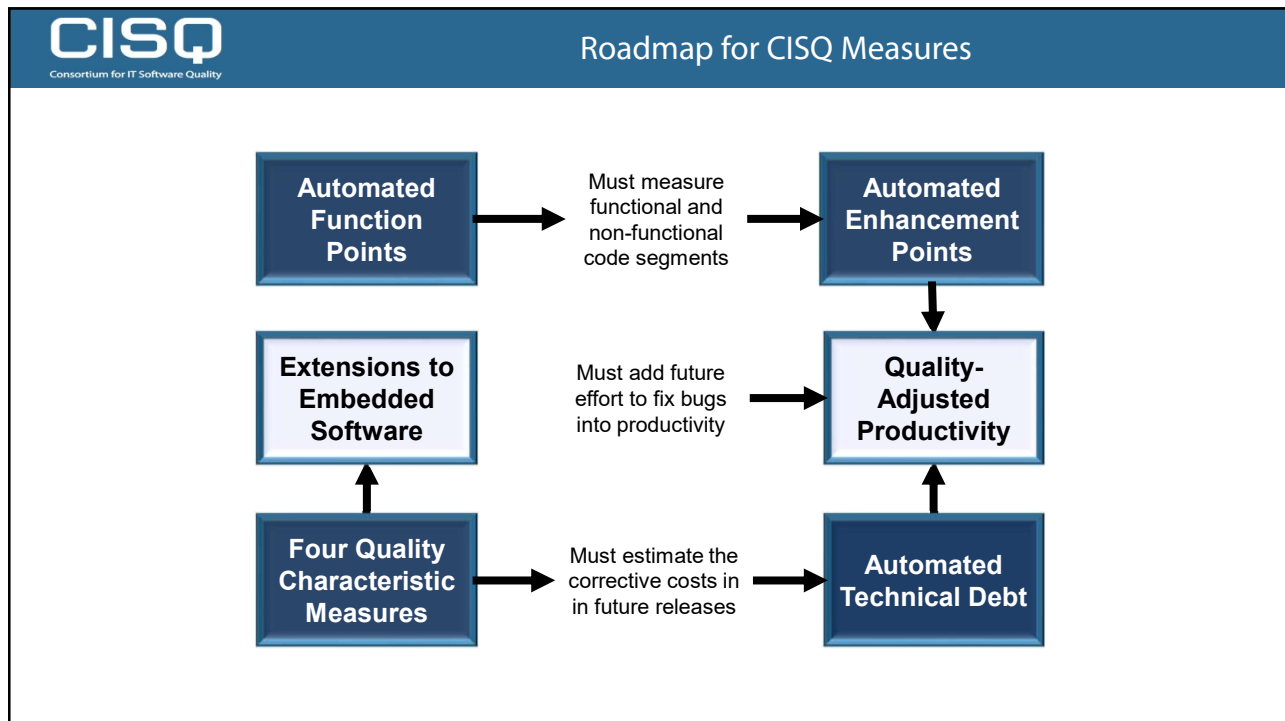
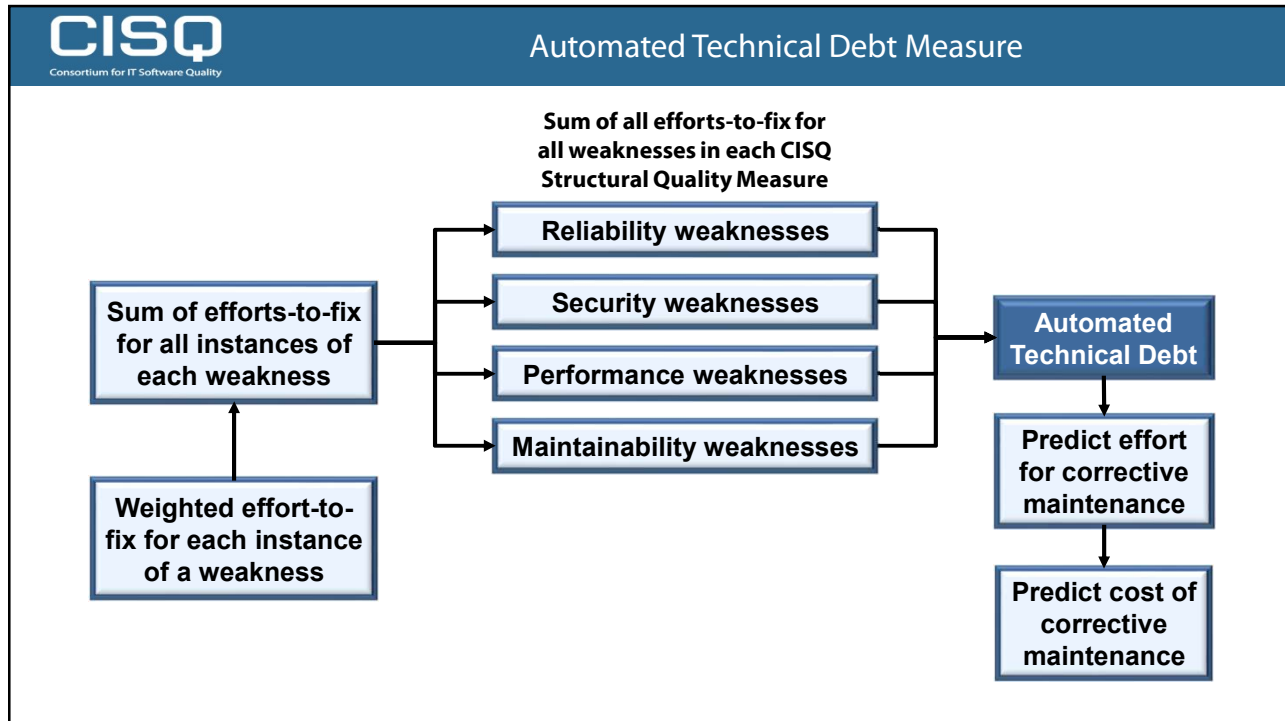
Robert Martin
MITRE

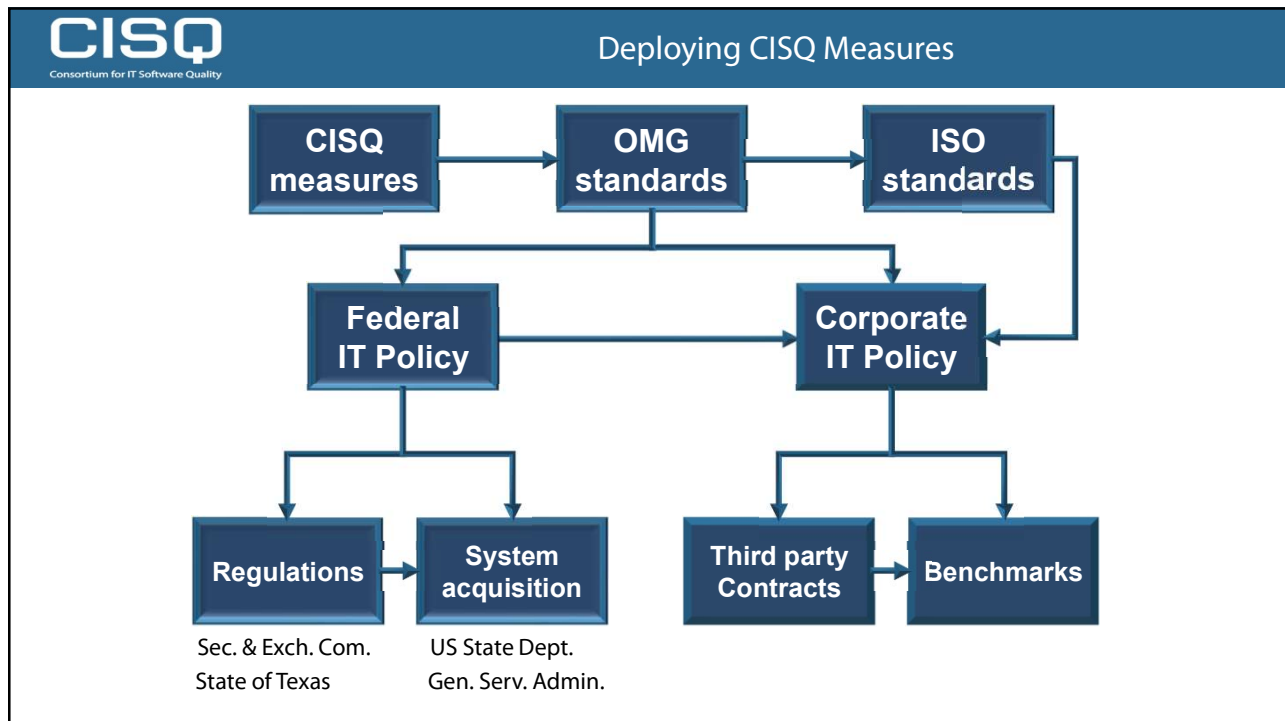
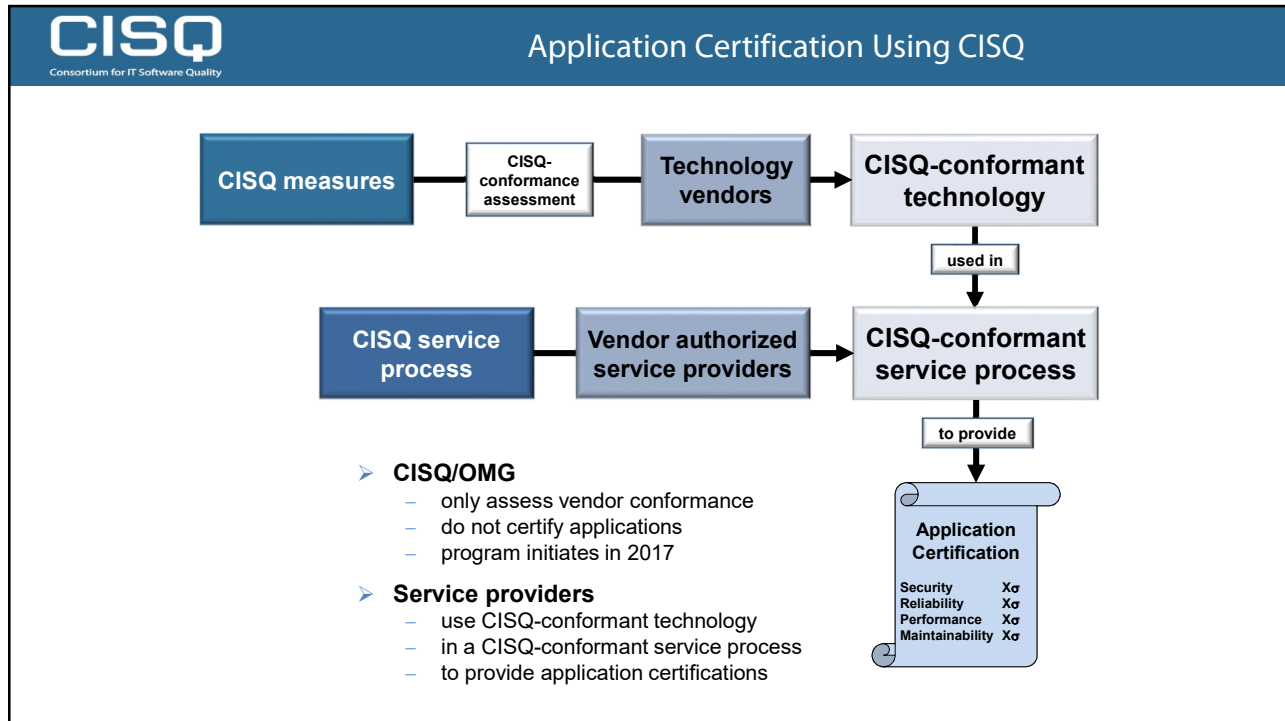


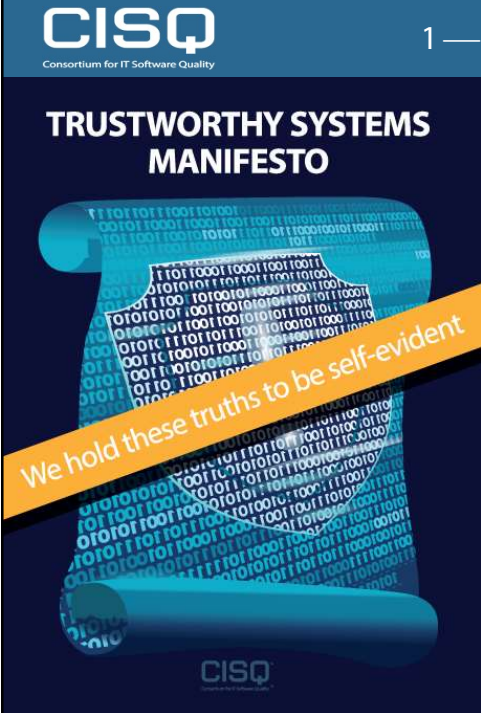
CWE
Common Weakness Enumeration
cwe.mitre.org











CISQ
Consortium for IT Software Quality

1 — Engineering Discipline in Process and Product

TRUSTWORTHY SYSTEMS MANIFESTO

We hold these truths to be self-evident

As a greater portion of mission, business, and safety critical functionality is committed to software-intensive systems, these systems become one of, if not the largest source of risk to enterprises and their customers. Since corporate executives are ultimately responsible for managing this risk, we establish the following principles to govern system development and deployment.

- 1. Engineering discipline in product and process**
- 2. Quality assurance to risk tolerance thresholds**
- 3. Traceable properties of system components**
- 4. Proactive defense of the system and its data**
- 5. Resilient and safe operations**

CISQ
Consortium for IT Software Quality