Software Security and Quality Issues in the Industrial Internet

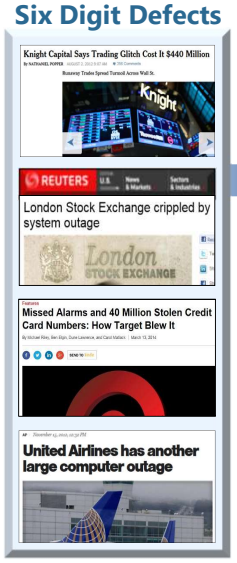
Dr. Bill Curtis
Executive Director

CISQ
Consortium for IT Software Quality

CISQ
Consortium for IT Software Quality

Why Measure IT Applications?

Six Digit Defects



now affect

- Board of Directors
- CEO, COO, CFO
- Business VPs
- Corporate Auditors
- CIO

accountable for

- Governance
- Risk management
- Risk measurement
- Brand protection
- Customer experience

Evaluate Application Quality with CISQ Measures

What is CISQ?

Consortium for IT Software Quality

Carnegie Mellon Software Engineering Institute

OMG Object Management Group

Co-founders

IT Executives → **CISQ** ← Technical Experts

OMG Special Interest Group

CISQ is chartered to define automatable measures of software size and quality that can be measured in the source code, and promote them to become Approved Specifications of the OMG®

CISQ Sponsors

Booz | Allen | Hamilton

Cognizant SYNOPSYS

CAST — Achieve Insight. Deliver Excellence.

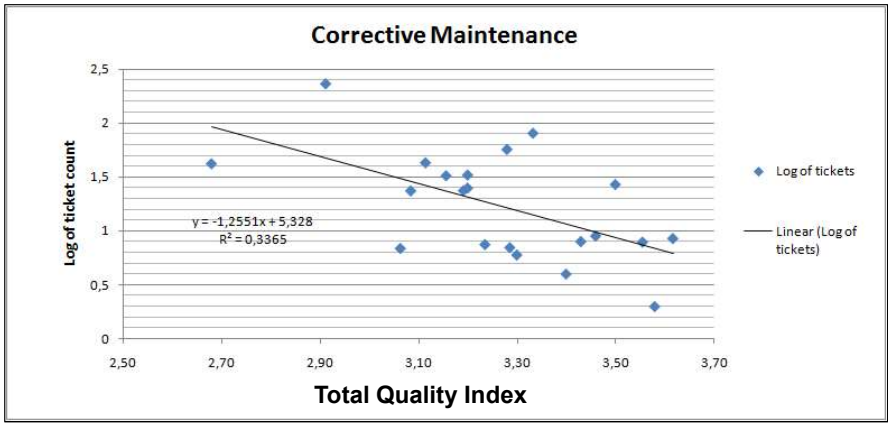
HUAWEI

2

Reducing Operational Incidents & Costs

Consortium for IT Software Quality

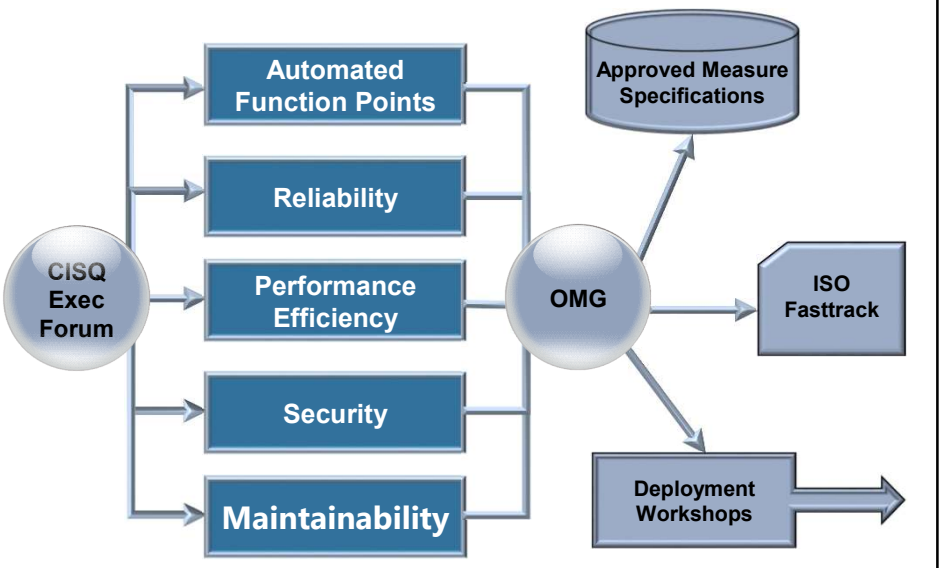
Study of structural quality measures and maintenance effort across 20 customers in a large global system integrator



TQI increase of .24 decreased corrective maintenance effort by 50%

4

CISQ/OMG Standards Process



3

Content of CISQ Measures

CISQ Quality Characteristic Measures		Example architectural and coding violations composing the CISQ measures
Security	22 violations (Top 25 CWEs)	• SQL injection • Cross-site scripting • Buffer overflow
Reliability	29 violations	• Empty exception block • Unreleased resources • Circular dependency
Performance Efficiency	15 violations	• Expensive loop operation • Un-indexed data access • Unreleased memory
Maintainability	20 violations	• Excessive coupling • Dead code • Hard-coded literals

5

The 22 CWEs in the Security Measure

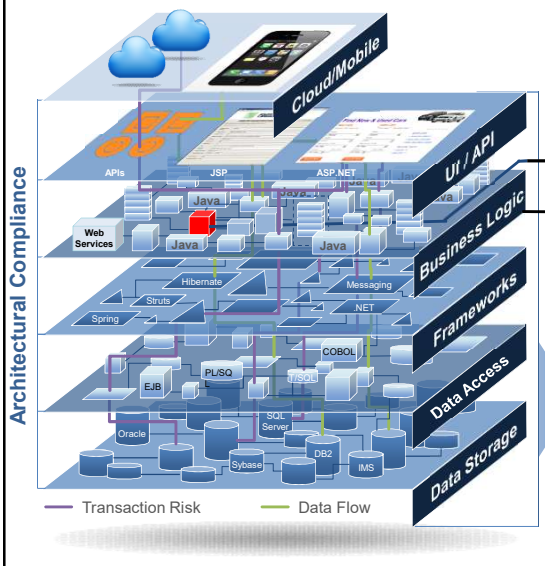
- CWE-22 Path Traversal Improper Input Neutralization
- CWE-78 OS Command Injection Improper Input Neutralization
- CWE-79 Cross-site Scripting Improper Input Neutralization
- CWE-89 SQL Injection Improper Input Neutralization
- CWE-120 Buffer Copy without Checking Size of Input
- CWE-129 Array Index 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

Common Weakness Enumeration
cwe.mitre.org

7

Modern Apps Are a Technology Stack



1 Unit Level
- Code style & layout
- Expression complexity
- Code documentation
- Class or program design
- Basic coding standards
- Developer level

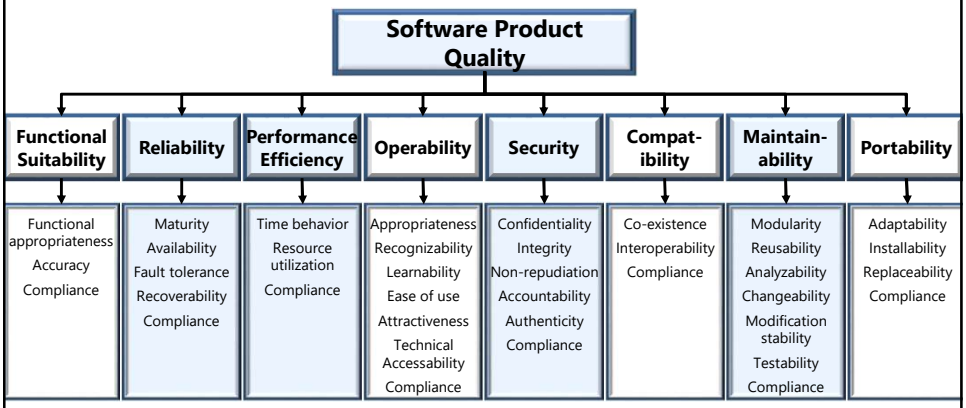
2 Technology Level
- Single language/technology layer
- Intra-technology architecture
- Intra-layer dependencies
- Inter-program invocation
- Security vulnerabilities
- Development team level

3 System Level
- Integration quality
- Architectural compliance
- Risk propagation
- Application security
- Resiliency checks
- Transaction integrity
- Function point
- Effort estimation
- Data access control
- SDK versioning
- Calibration across technologies
- IT organization level

8

How Do CISQ Measures Relate to ISO?

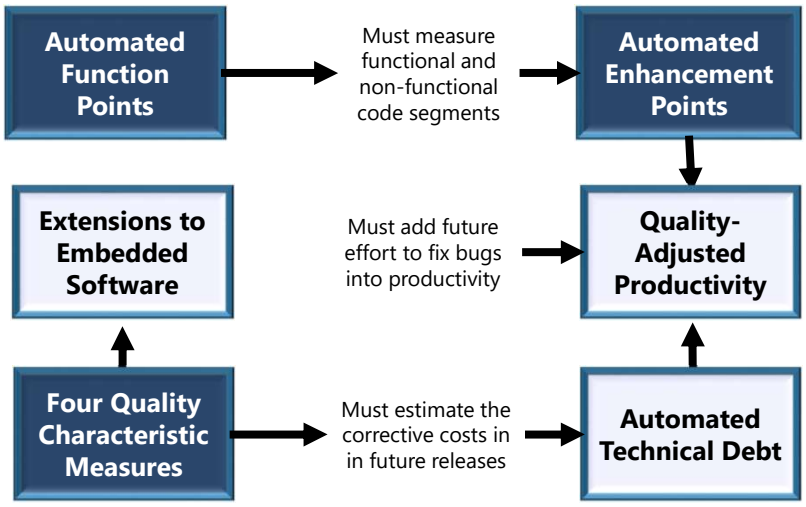
- ISO 25000 series replaces ISO/IEC 9126 (Parts 1-4)
- ISO 25010 defines quality characteristics and sub-characteristics
- CISQ conforms to ISO 25010 quality characteristic definitions
- ISO 25023 defines measures, but not at the source code level
- CISQ supplements ISO 25023 with source code level measures



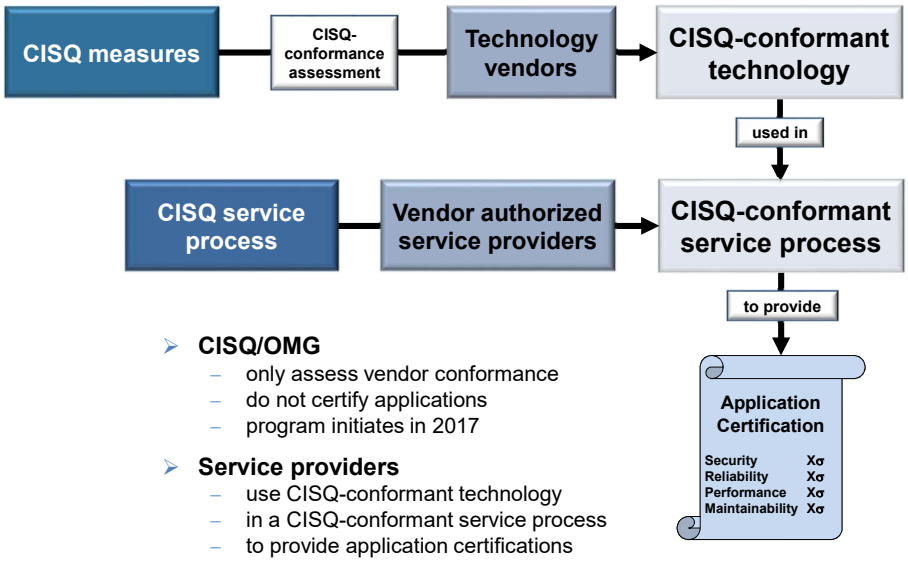
CISQ automated quality characteristic measures highlighted in blue

9

Emerging CISQ Measures



App Certification Using CISQ



- **CISQ/OMG**
  - only assess vendor conformance
  - do not certify applications
  - program initiates in 2017
- **Service providers**
  - use CISQ-conformant technology
  - in a CISQ-conformant service process
  - to provide application certifications

12

Join CISQ ! www.it-cisq.org

15