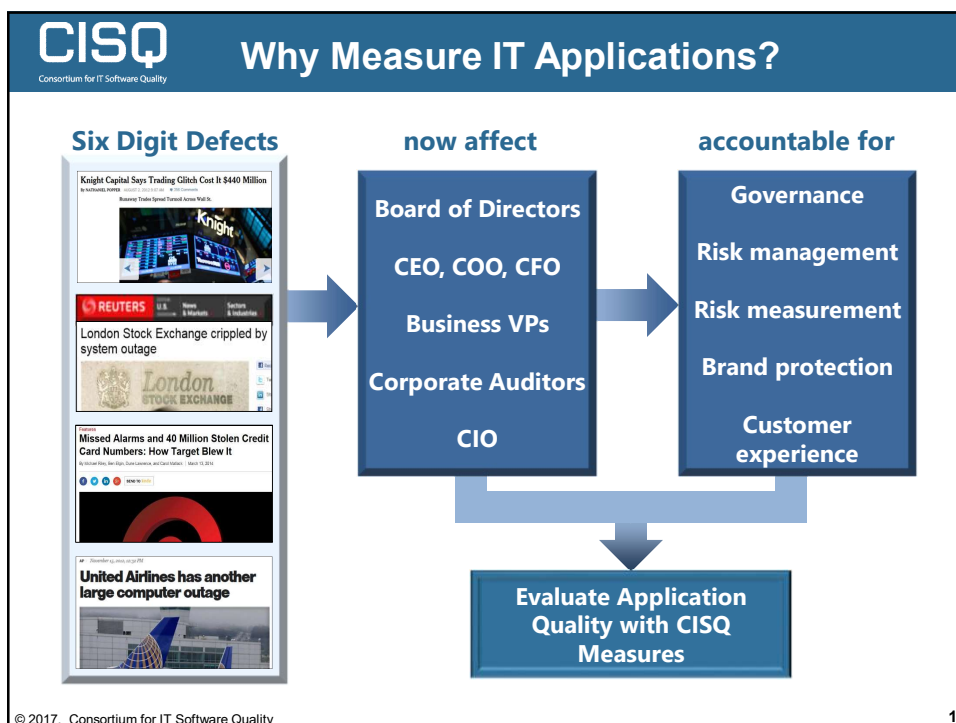# Advances in Software Quality Measurement

Dr. Bill Curtis
Executive Director

CISQ
Consortium for IT Software Quality

CISQ
Consortium for IT Software Quality

Why Measure IT Applications?

Six Digit Defects

Knight Capital Says Trading Glitch Cost It $440 Million
By NATHANIEL POPPER AUGUST 2, 2012 8:37 AM 193 Comments
Runaway Trades Spread Turmoil Across Wall St.

REUTERS
London Stock Exchange crippled by system outage

Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It
By Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack | March 13, 2014

United Airlines has another large computer outage

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

1

What is CISQ?

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
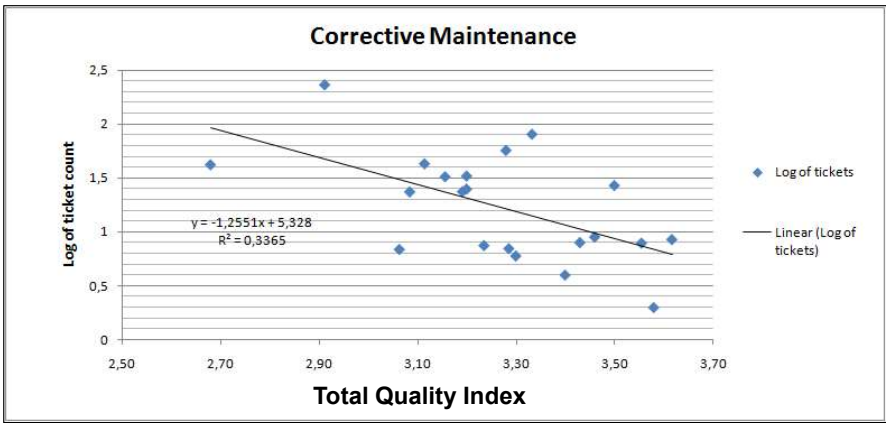
Reducing Operational Incidents & Costs

CISQ Consortium for IT Software Quality

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

Corrective Maintenance

$y = -1,2551x + 5,328$
$R^2 = 0,3365$

- Log of tickets
- Linear (Log of tickets)

Log of ticket count (y-axis: 0 to 2,5)

Total Quality Index (x-axis: 2,50 to 3,70)

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

4

CISQ/OMG Standards Process

CISQ Consortium for IT Software Quality

- CISQ Exec Forum
  - Automated Function Points
  - Reliability
  - Performance Efficiency
  - Security
  - Maintainability
- OMG
  - Approved Measure Specifications
  - ISO Fasttrack
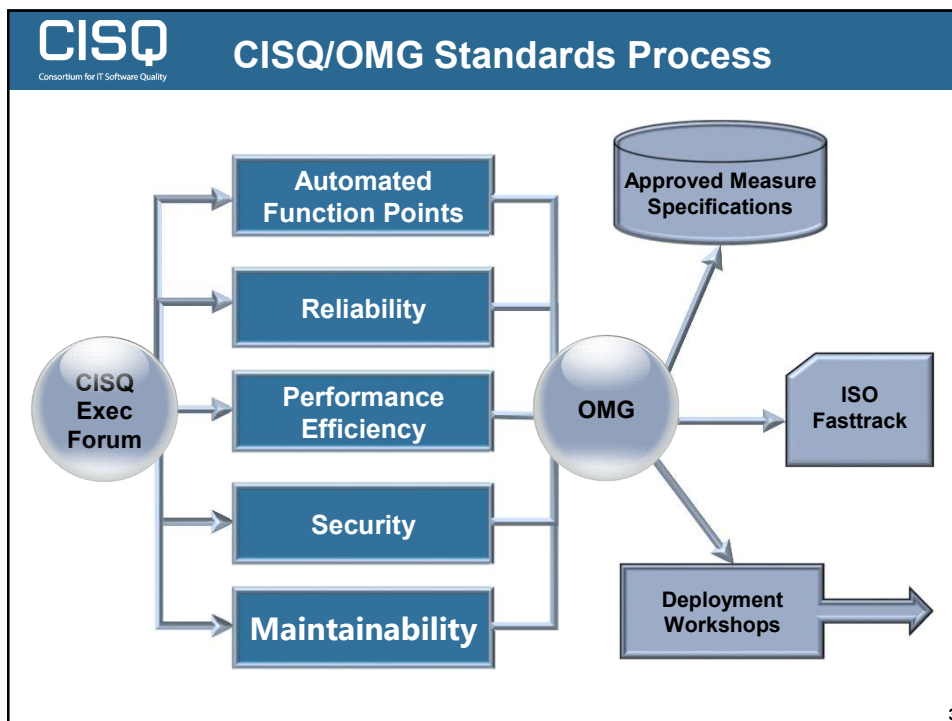 - Deployment Workshops

3

Automated Function Points

CISQ Consortium for IT Software Quality

- **OMG Supported Specification for Automated Function Points**

- **Mirrors IFPUG counting guidelines, but automatable**

- **Specification developed by international team led by David Herron of David Consulting Group**

Date: January 2014

OMG
OBJECT MANAGEMENT GROUP

Automated Function Points (AFP)

Version 1.0

OMG Document Number: formal/2014-01-03
Standard document URL: http://www.omg.org/spec/AFP
Machine consumable files:
      Normative: http://www.omg.org/spec/AFP/20120901/AutomatedFunctionPoint.xmi

Addison-Wesley Information Technology Series

Function Point Analysis

Measurement Practices for Successful Software Projects

David Garmus
David Herron
Foreword by Capers Jones

4

Content of CISQ Measures

CISQ
Consortium for IT Software Quality

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

CISQ
Consortium for IT Software Quality

- **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
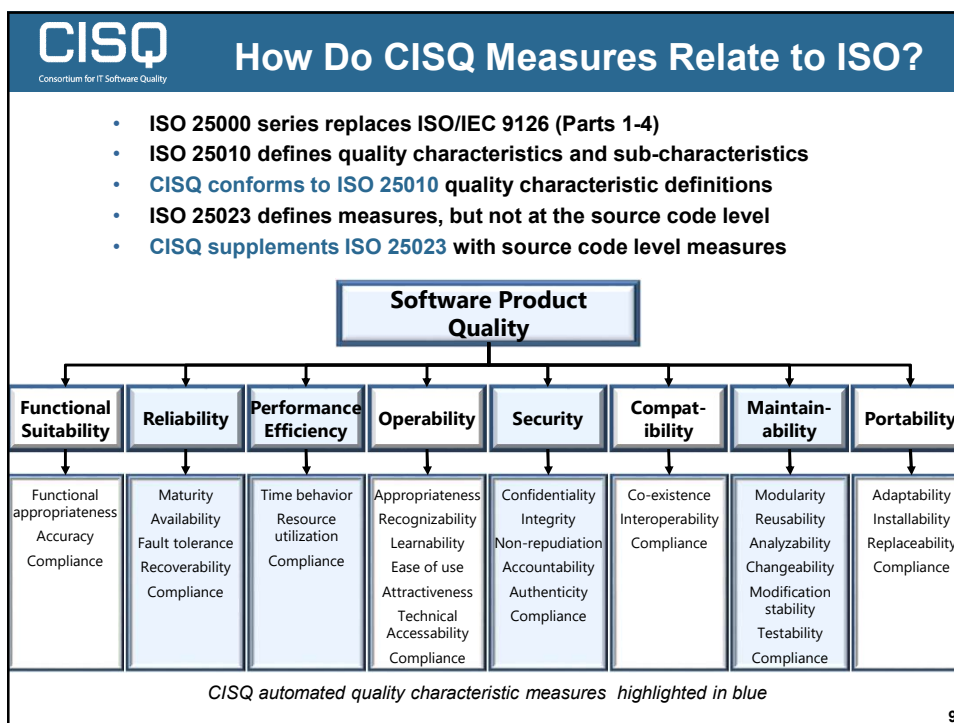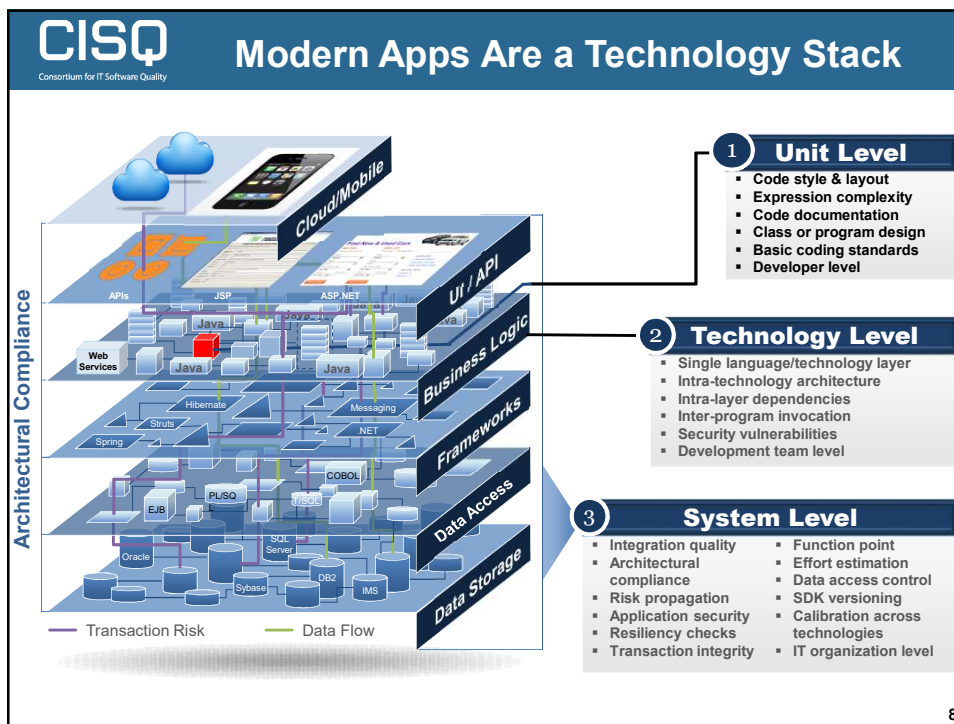- **CWE-835** Loop with Unreachable Exit Condition ('Infinite Loop')

Robert Martin
MITRE

CWE

Common Weakness Enumeration
cwe.mitre.org

7

Modern Apps Are a Technology Stack

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

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

System Level
3
- 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

— Transaction Risk   — Data Flow

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

Software Product Quality

Functional Suitability	Reliability	Performance Efficiency	Operability	Security	Compat-ibility	Maintain-ability	Portability
Functional appropriateness	Maturity	Time behavior	Appropriateness	Confidentiality	Co-existence	Modularity	Adaptability
Accuracy	Availability	Resource utilization	Recognizability	Integrity	Interoperability	Reusability	Installability
Compliance	Fault tolerance	Compliance	Learnability	Non-repudiation	Compliance	Analyzability	Replaceability
	Recoverability		Ease of use	Accountability		Changeability	Compliance
	Compliance		Attractiveness	Authenticity		Modification stability	
			Technical Accessability	Compliance		Testability	
			Compliance			Compliance	

CISQ automated quality characteristic measures highlighted in blue

9

CISQ in Service Level Agreements

CISQ — Consortium for IT Software Quality

Evaluate Product Quality against Targets in Quality Level Agreements

Outsourcer	Automated Function Points	Reliability	Performance Efficiency	Security	Maintainability
VENDOR 1	245	3.16	2.34	3.01	1.99
VENDOR 2	628	2.78	2.78	3.12	2.34
VENDOR 3	931	1.67	3.54	2.98	1.76
VENDOR 4	659	3.12	3.11	2.79	3.11
VENDOR 5	86	2.56	2.88	3.03	2.56
VENDOR 6	1047	3.76	2.89	2.97	2.55

Monitor and Manage Service Provider Performance

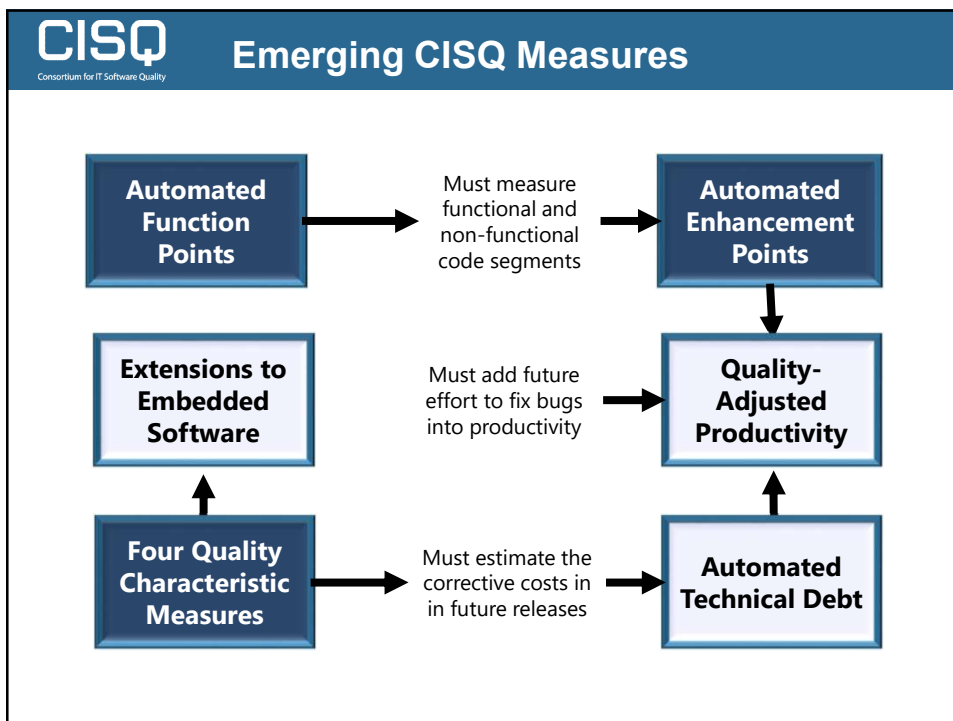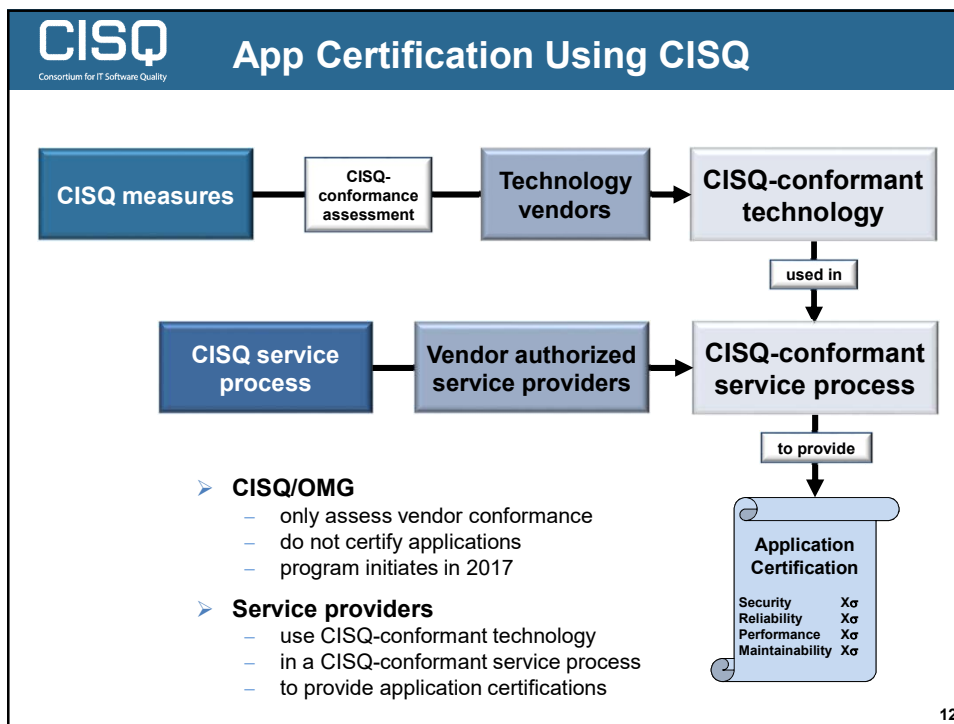**TECHNICAL CODE QUALITY** — AVERAGE TQI FEBRUARY 2012-JUNE 2014

Mean Time to Repair — **TECHNICAL DEBT** — PRE-PRODUCTION FEBRUARY 2012-JUNE 2014 — 2012.02 / 2012.06

Productivity — **COST EFFECTIVENESS** — COST PER FUNCTION POINT / ENHANCEMENT FEBRUARY 2012-JUNE 2014 — 2012.02 / 2012.06

11

Emerging CISQ Measures

CISQ — Consortium for IT Software Quality

Automated Function Points → Must measure functional and non-functional code segments → **Automated Enhancement Points**

Extensions to Embedded Software — Must add future effort to fix bugs into productivity → **Quality-Adjusted Productivity**

Four Quality Characteristic Measures → Must estimate the corrective costs in in future releases → **Automated Technical Debt**

App Certification Using CISQ

CISQ measures → CISQ-conformance assessment → Technology vendors → CISQ-conformant technology

used in

CISQ service process → Vendor authorized service providers → CISQ-conformant service process

to provide

Application Certification

Security   Xσ
Reliability   Xσ
Performance Xσ
Maintainability Xσ

➢ **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