Measuring the Cybersecurity Risk of Software-Intensive Systems

Marc Jones
Director, CISQ Federal Outreach

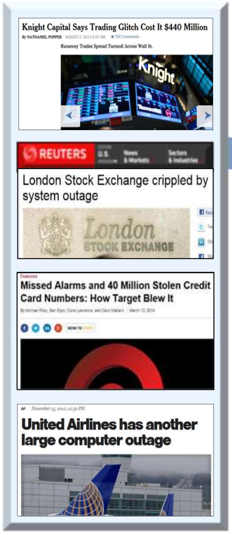
CISQ
Consortium for IT Software Quality

International Standards for Automating Software Size and Structural Quality Measurement

CISQ
Consortium for IT Software Quality

Nine-Digit Glitches

Nine Digit Glitches



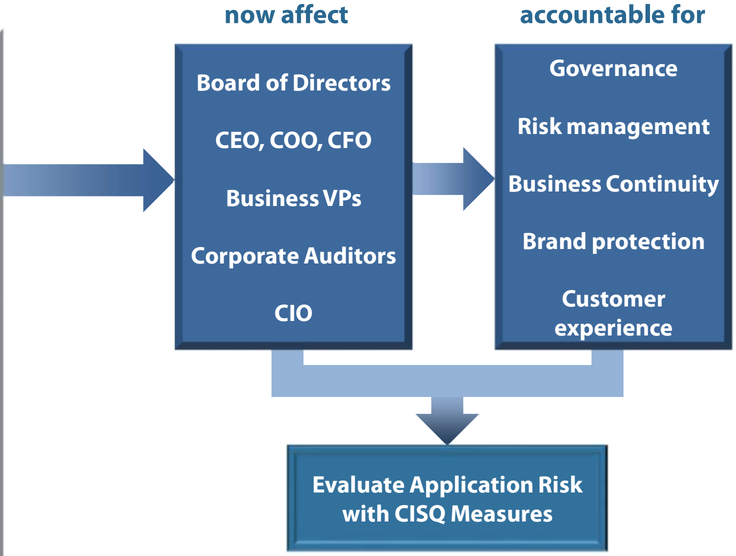
Knight Capital Says Trading Glitch Cost It $440 Million
By NATHANIEL POPPER AUGUST 2, 2012 9:07 AM 356 Comments
Runaway Trades Spread Turmoil Across Wall St.

REUTERS U.S. News & Markets Sectors & Industries

London Stock Exchange crippled by system outage

Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It

AP November 15, 2012, 12:32 PM
United Airlines has another large computer outage



now affect

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

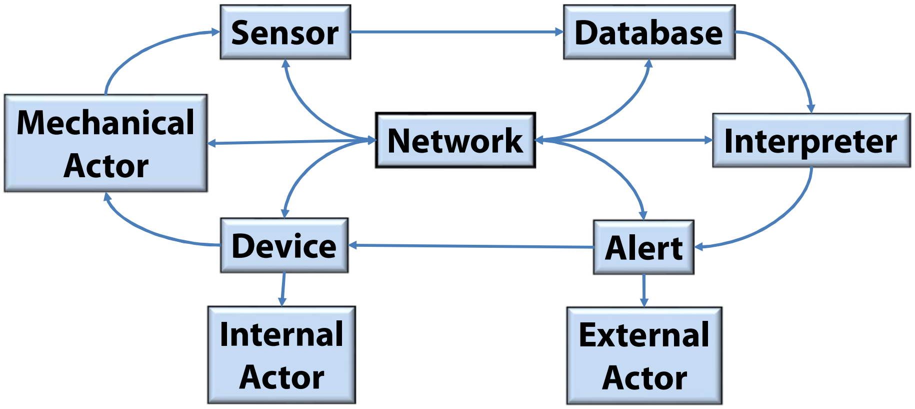
accountable for

- Governance
- Risk management
- Business Continuity
- Brand protection
- Customer experience

Evaluate Application Risk with CISQ Measures

© 2018 Consortium for IT Software Quality (CISQ) www.it-cisq.org

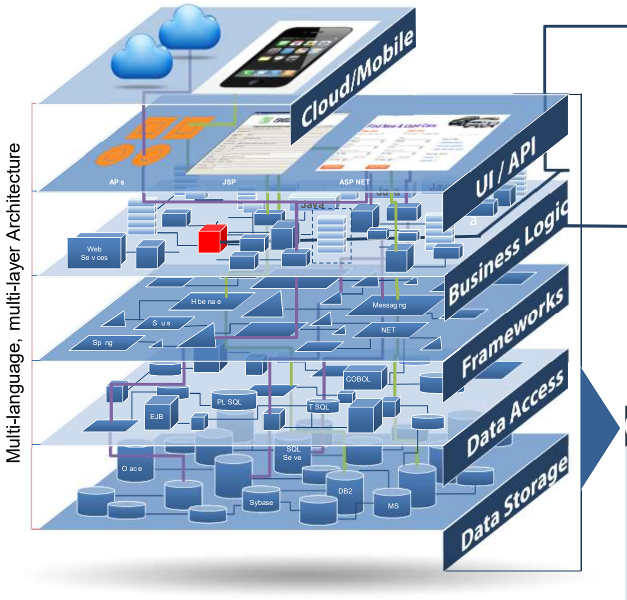
Security Challenges in IoT Systems



- Broad attack surface with rapid propagation across components
- Components developed by different organizations
- Lack of shared cybersecurity information on component weaknesses
- Reliance on process certifications instead of software analysis

© 2018 Consortium for IT Software Quality (CISQ) www.it-cisq.org

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

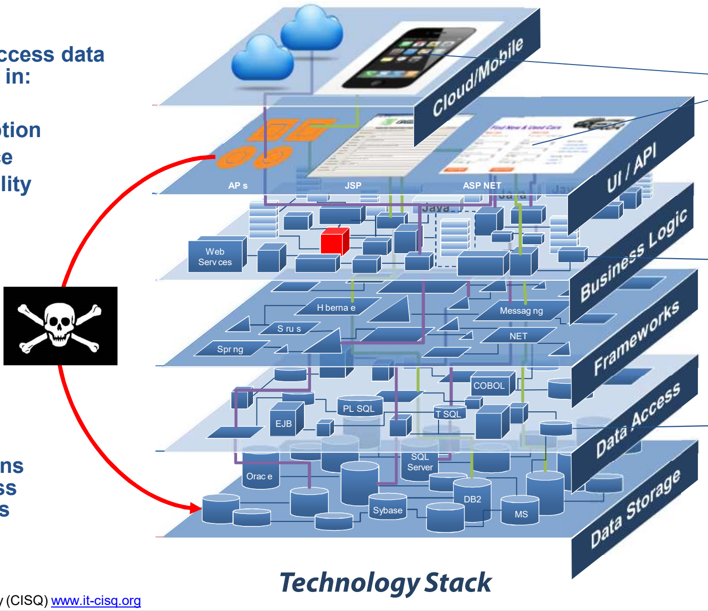
- Multiple languages
- Architectural compliance
- Risk propagation
- Application security
- Resiliency checks
- Transaction integrity
- Function points
- Integration quality
- Data access control
- SDK versioning
- Calibration across technologies
- IT organization level

2© 2018 Consortium for IT Software Quality (CISQ) www.it-cisq.org

CISQ Security Analysis Must Be System-Wide

Skipping layers to access data can cause problems in:

- Security
- Data corruption
- Performance
- Maintainability



User entry

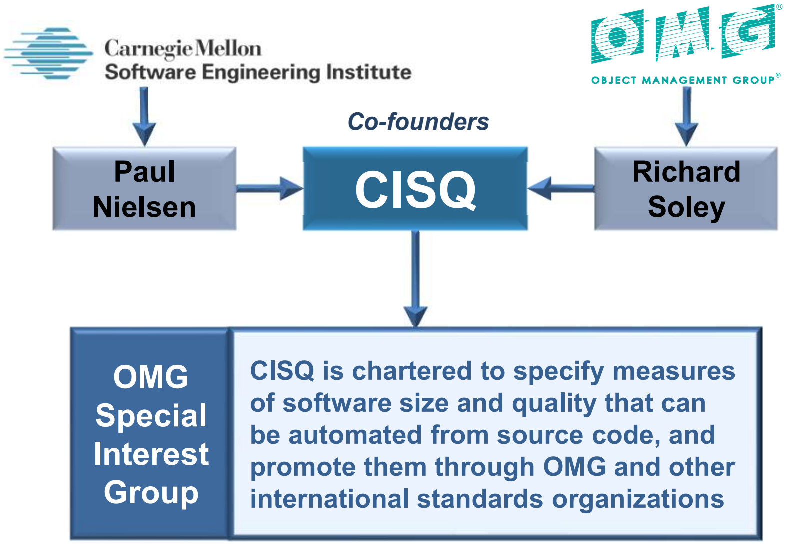
User & input authentication

Data access manager

Detection requires analyzing transactions and data flows across languages and layers

Technology Stack

CISQ What Is CISQ ?



Carnegie Mellon Software Engineering Institute

OMG OBJECT MANAGEMENT GROUP

Co-founders

Paul Nielsen

CISQ

Richard Soley

OMG Special Interest Group

CISQ is chartered to specify measures of software size and quality that can be automated from source code, and promote them through OMG and other international standards organizations

CISQ Sponsors

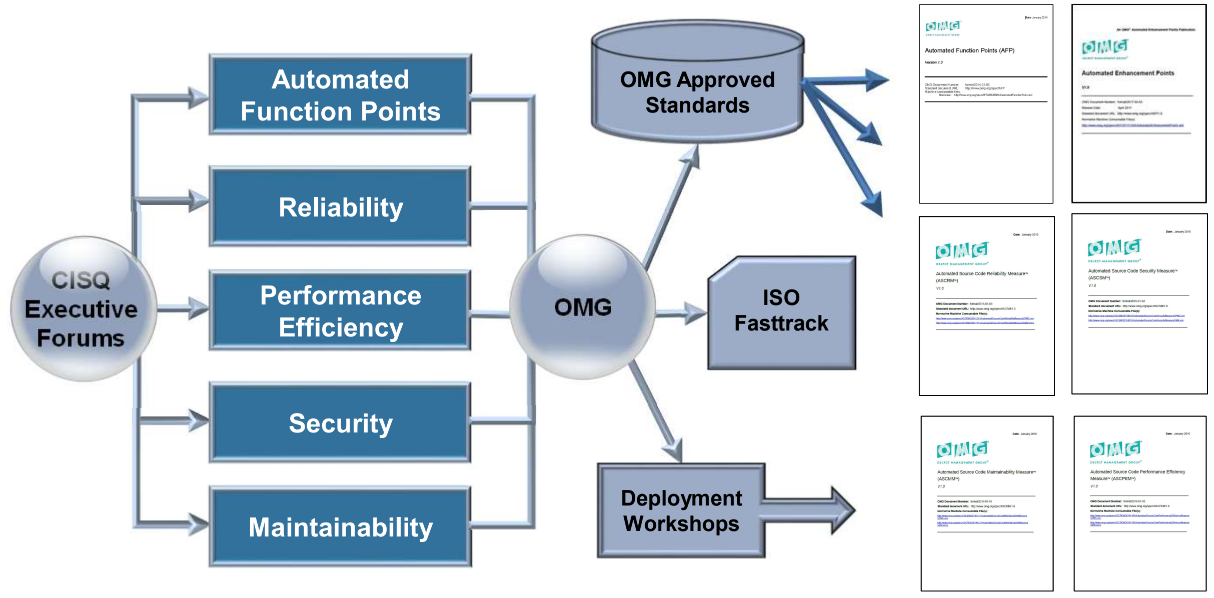
Cognizant, SYNOPSYS, Tech Mahindra, SHPI, CAST, CGI, NORTHROP GRUMMAN

CISQ Partners

Gartner, QuEST FORUM, FORRESTER, IAOP, ITAAC, TECHWELL, MAKING SOFTWARE BETTER

CISQ
Consortium for IT Software Quality

CISQ/OMG Standards Process



© 2018 Consortium for IT Software Quality (CISQ) www.it-cisq.org

CISQ
Consortium for IT Software Quality

CISQ Structural Quality Measures

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

An international team of experts selected the weaknesses to include in CISQ measures based on the severity of their impact on operational problems or cost of ownership.

Only weaknesses considered severe enough that they must be remediated were included in the CISQ measures.

CISQ Structural Quality measures are currently being extended to embedded systems software.

© 2018 Consortium for IT Software Quality (CISQ) www.it-cisq.org

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')

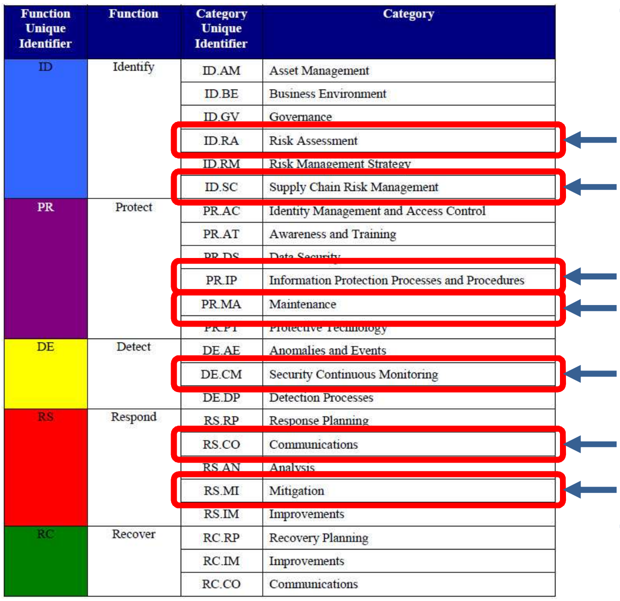
Robert Martin
MITRE

CWE
Common Weakness Enumeration
cwe.mitre.org

Update to CISQ measures:

- Extensions for embedded
- Additional critical weaknesses
- Expected 2H 2019
- CWE Parent-child structure:
  - 34 parents
  - 41 children

CISQ and the NIST Cybersecurity Framework



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

The CISQ Security measure (and others) can be used in numerous processes of the NIST Cybersecurity Framework. Some examples:

Empirical risk tolerance thresholds for software security

Contractual SLAs and audits for software security

Evaluation of software assets for security weaknesses

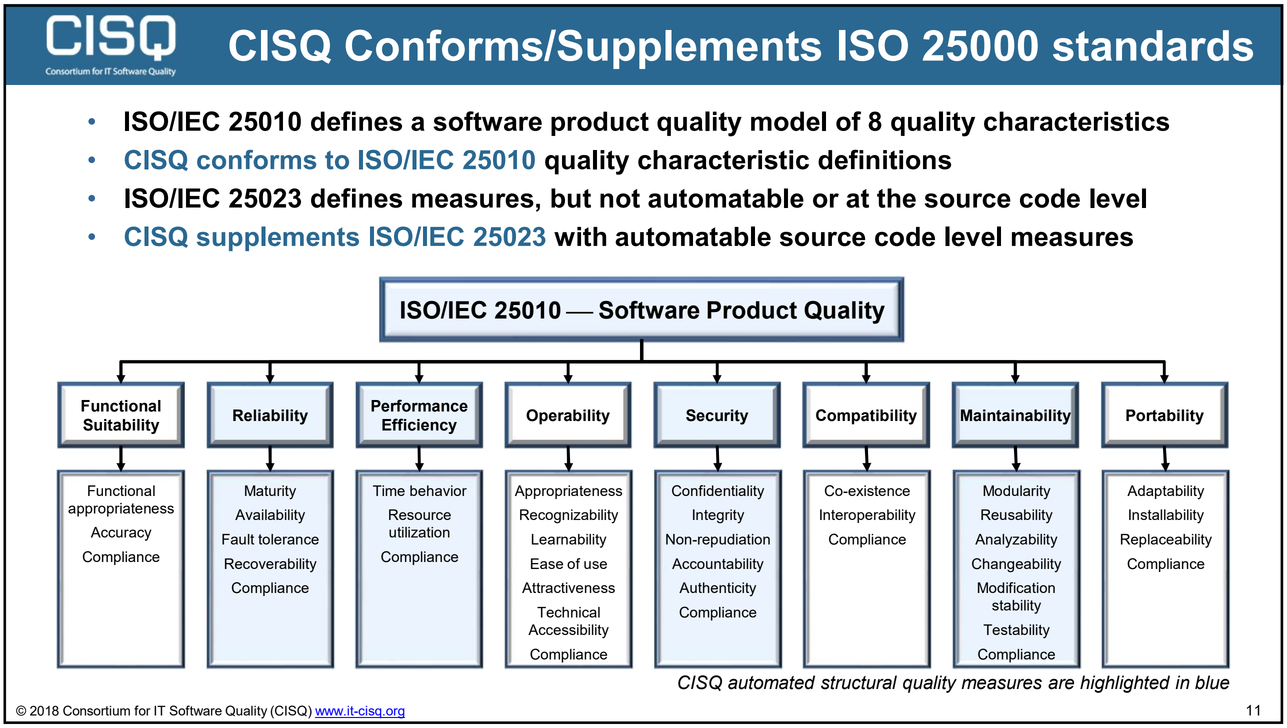
Continual improvement of software security

Periodic scans for software weaknesses

Software security and weakness data are shared

Security weaknesses are identified and mitigated

The CISQ structural quality measures play an important requirements and verification role for 'Build Security In' approaches to cybersecurity



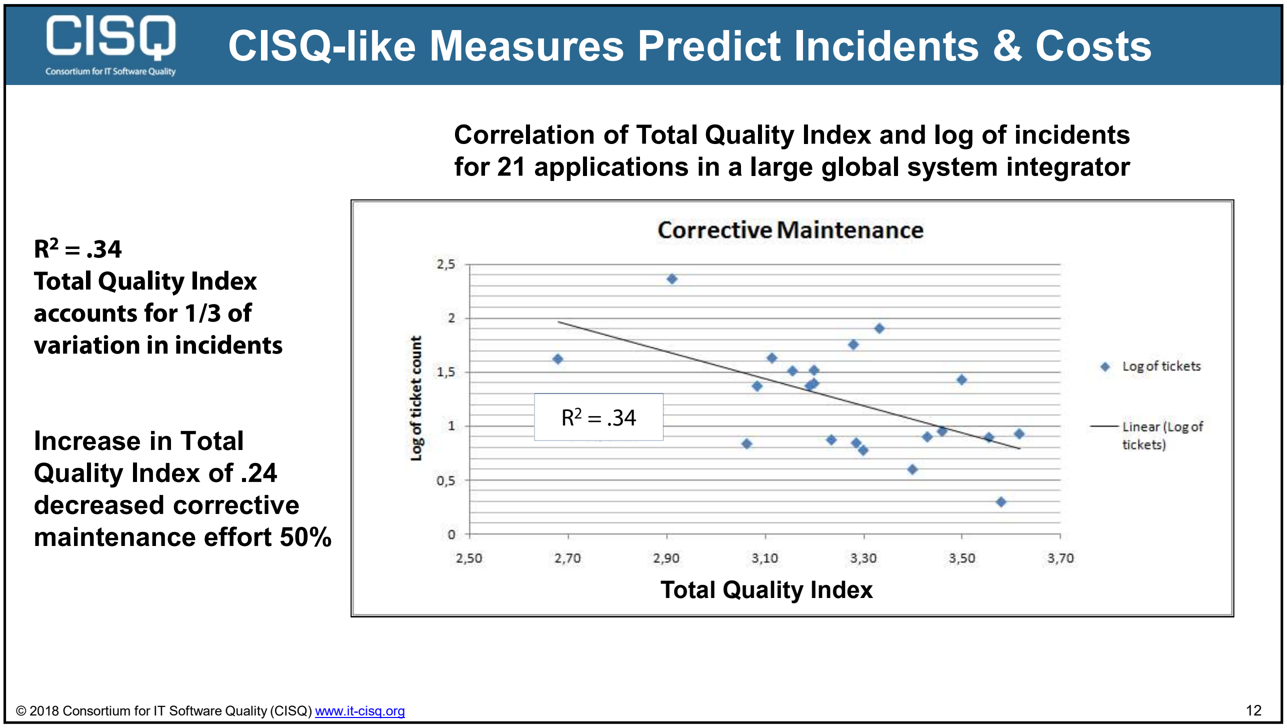
CISQ Conforms/Supplements ISO 25000 standards

- ISO/IEC 25010 defines a software product quality model of 8 quality characteristics
- CISQ conforms to ISO/IEC 25010 quality characteristic definitions
- ISO/IEC 25023 defines measures, but not automatable or at the source code level
- CISQ supplements ISO/IEC 25023 with automatable source code level measures

ISO/IEC 25010 — Software Product Quality

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

CISQ automated structural quality measures are highlighted in blue

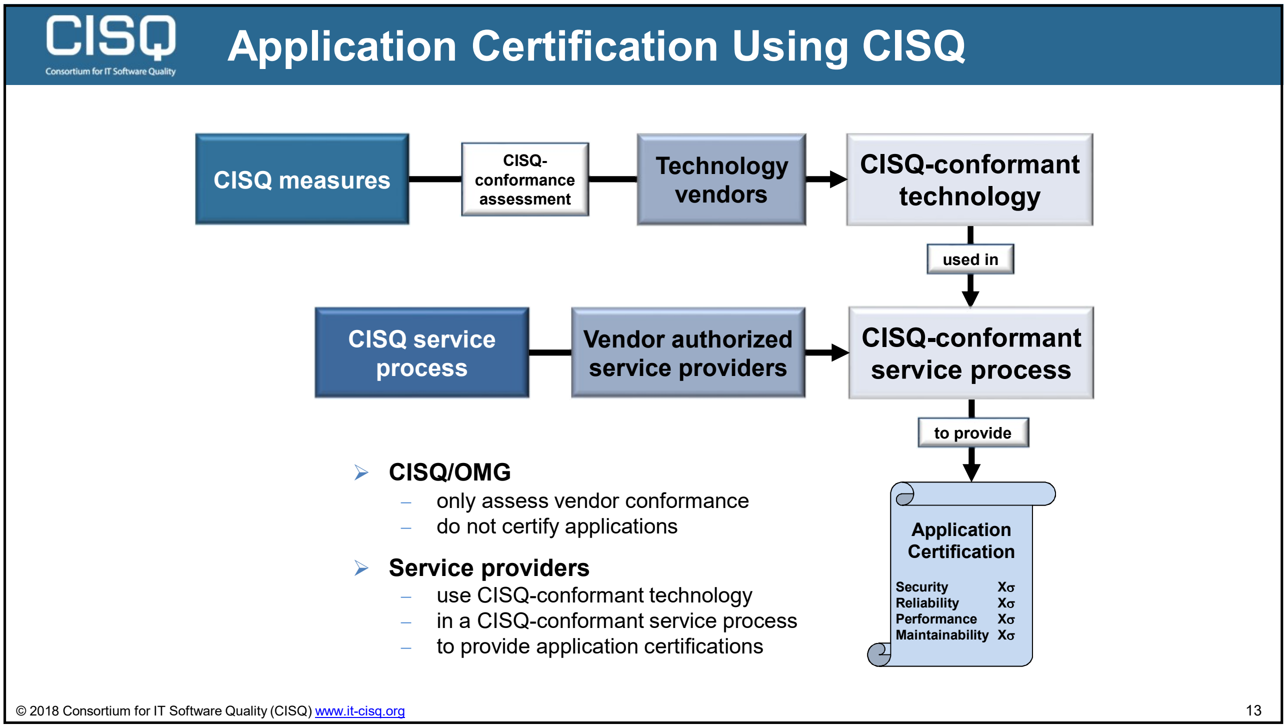


CISQ-like Measures Predict Incidents & Costs

Correlation of Total Quality Index and log of incidents for 21 applications in a large global system integrator

R^2 = .34
Total Quality Index accounts for 1/3 of variation in incidents

Increase in Total Quality Index of .24 decreased corrective maintenance effort 50%



Application 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

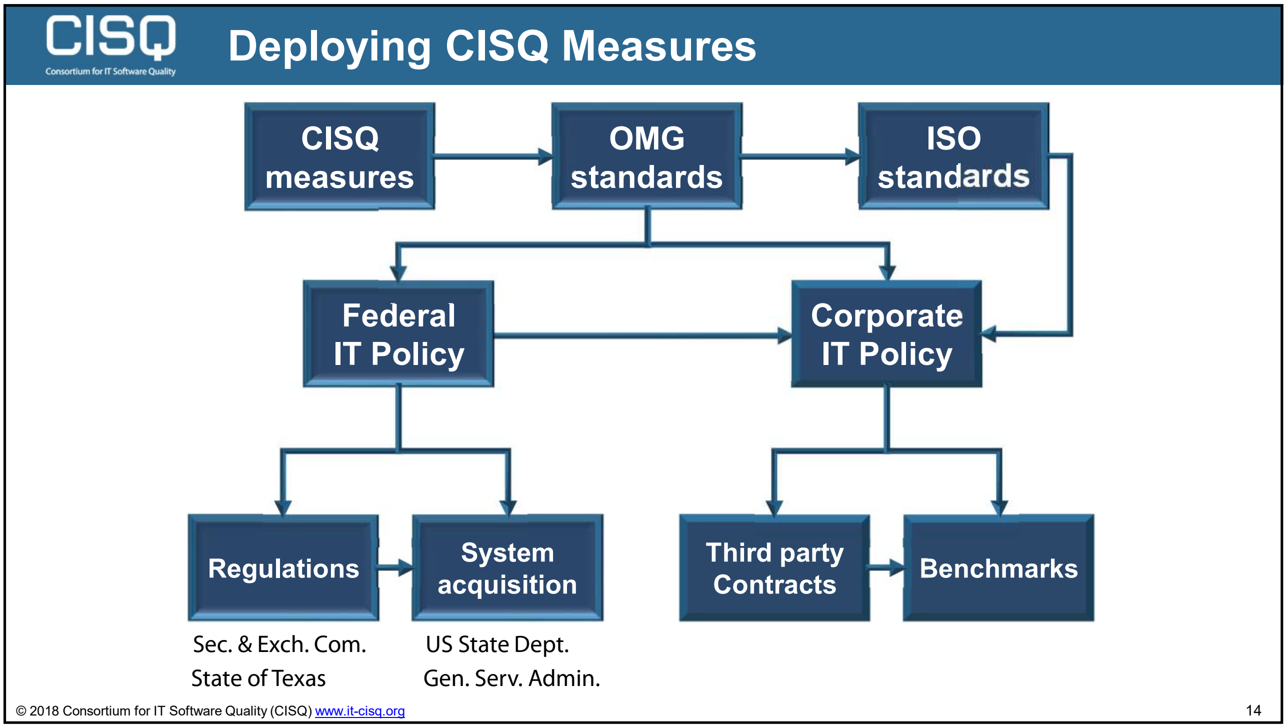
to provide ↓

Application Certification

Security	Xσ
Reliability	Xσ
Performance	Xσ
Maintainability	Xσ

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

© 2018 Consortium for IT Software Quality (CISQ) www.it-cisq.org



Deploying CISQ Measures

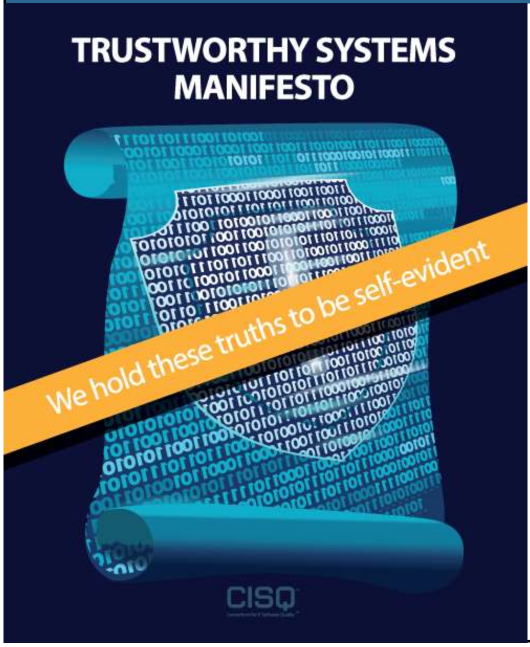
Sec. & Exch. Com.
State of Texas

US State Dept.
Gen. Serv. Admin.

© 2018 Consortium for IT Software Quality (CISQ) www.it-cisq.org

CISQ
Consortium for IT Software Quality

Trustworthy Systems Manifesto


TRUSTWORTHY SYSTEMS MANIFESTO
We hold these truths to be self-evident
CISQ

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

CISQ Membership Is Free — www.it-cisq.org

Standards to Automate Software Measurement

The Consortium for IT Software Quality™ (CISQ™) is an IT leadership group that develops international standards for automating the measurement of software size and structural quality from the source code. The standards written by CISQ enable IT and business leaders to measure the risk IT applications pose to the business, as well as estimate the cost of ownership. CISQ was co-founded by the Object Management Group® (OMG®) and Software Engineering Institute (SEI) at Carnegie Mellon University.

Watch the September 10 webinar: Expecting Secure, High-Quality Software: Mitigating Risks throughout the Lifecycle with Joe Jarzombek, Synopsys

Visit the IT Modernization Best Practices Repository with resources from the Cyber Resilience Summit series.

CISQ Sponsors

CYBER RESILIENCE SUMMIT

The Crossroads of Modernization and Cybersecurity

OCTOBER 16, 2018

ARMY NAVY COUNTRY CLUB, ARLINGTON, VA

Over 2000 individual members from large software-intensive organizations:

accenture, U.S. Department of Homeland Security, IBM, AXA, at&t, amazon, Infosys, BOSCH, ISG, BOEING, aetna, John Deere, Booz | Allen | Hamilton, Credit Suisse, Duke Energy, IAOP, Allianz, Gartner, Atos, citi, Capital One, DreamWorks, Huawei, Capgemini, Dell, FedEx, Discovery Health, ca technologies, DCG, Cisco, Fidelity Investments, HCL, CenturyLink, MITRE, Barclays

© 2018 Consortium for IT Software Quality (CISQ) www.it-cisq.org