Measuring the Cybersecurity Risk of Software-Intensive Systems

Marc Jones

Director, CISQ Federal Outreach

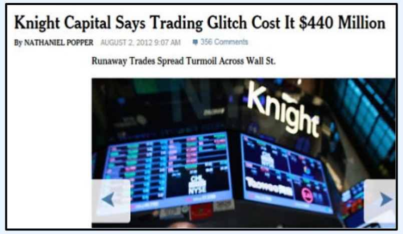
CISQ Consortium for IT Software Quality

International Standards for Automating Software Size and Structural Quality Measurement

CISQ
Consortium for IT Software Quality

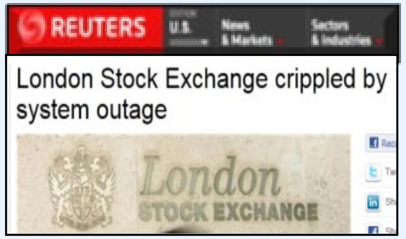
The Nine-Digit Glitch

Nine Digit Glitches

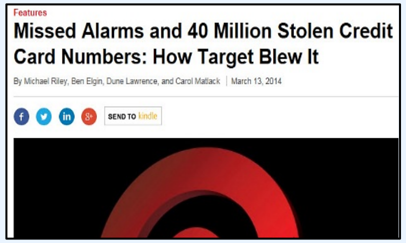

Knight Capital Says Trading Glitch Cost It $440 Million

By NATHANIEL POPPER AUGUST 2, 2012 9:07 AM 356 Comments

Runaway Trades Spread Turmoil Across Wall St.

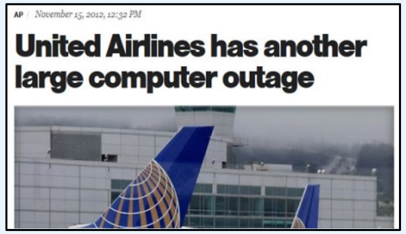


London Stock Exchange crippled by system outage

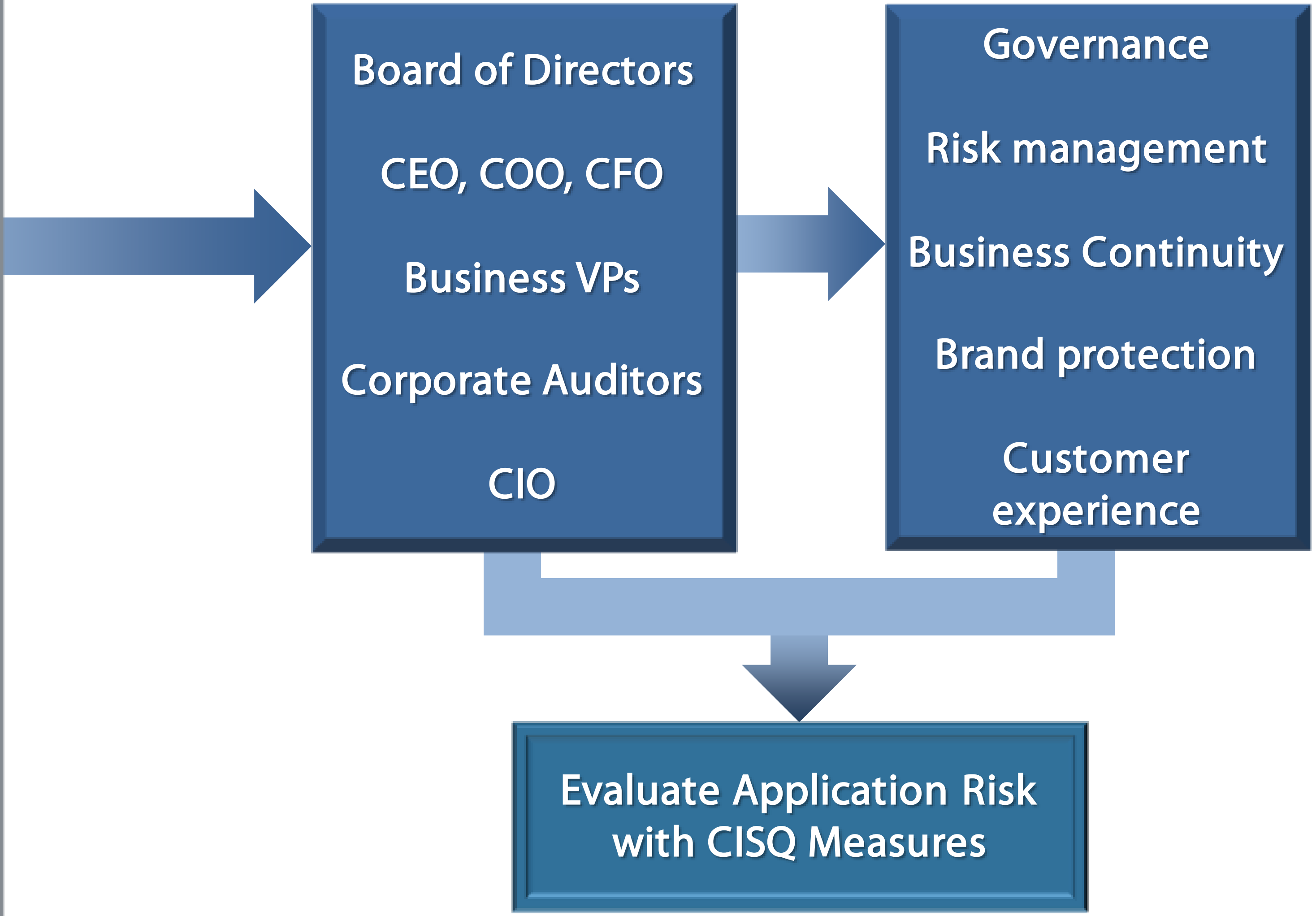

Features

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


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

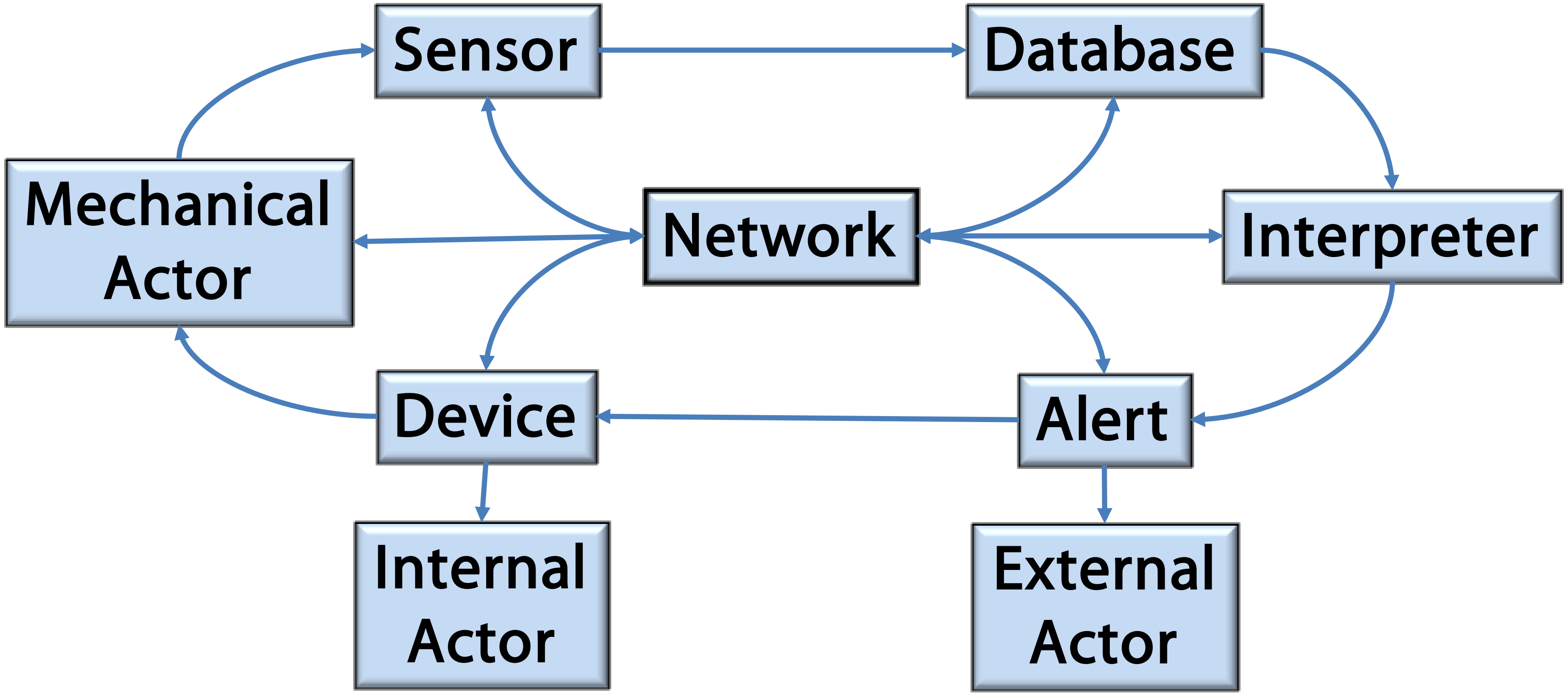
Customer experience

Evaluate Application Risk with CISQ Measures

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

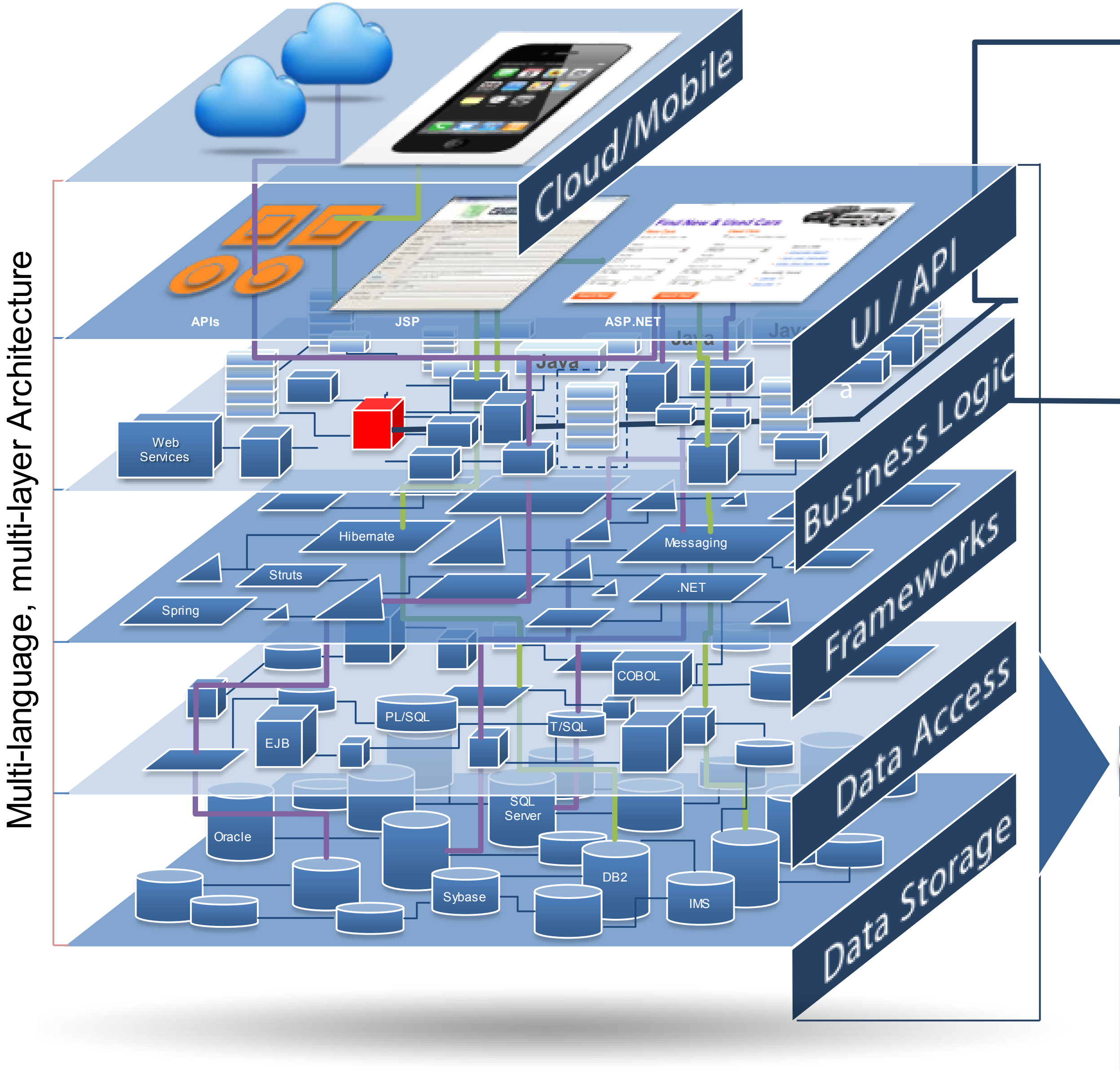
CISQ
Consortium for IT Software Quality

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

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

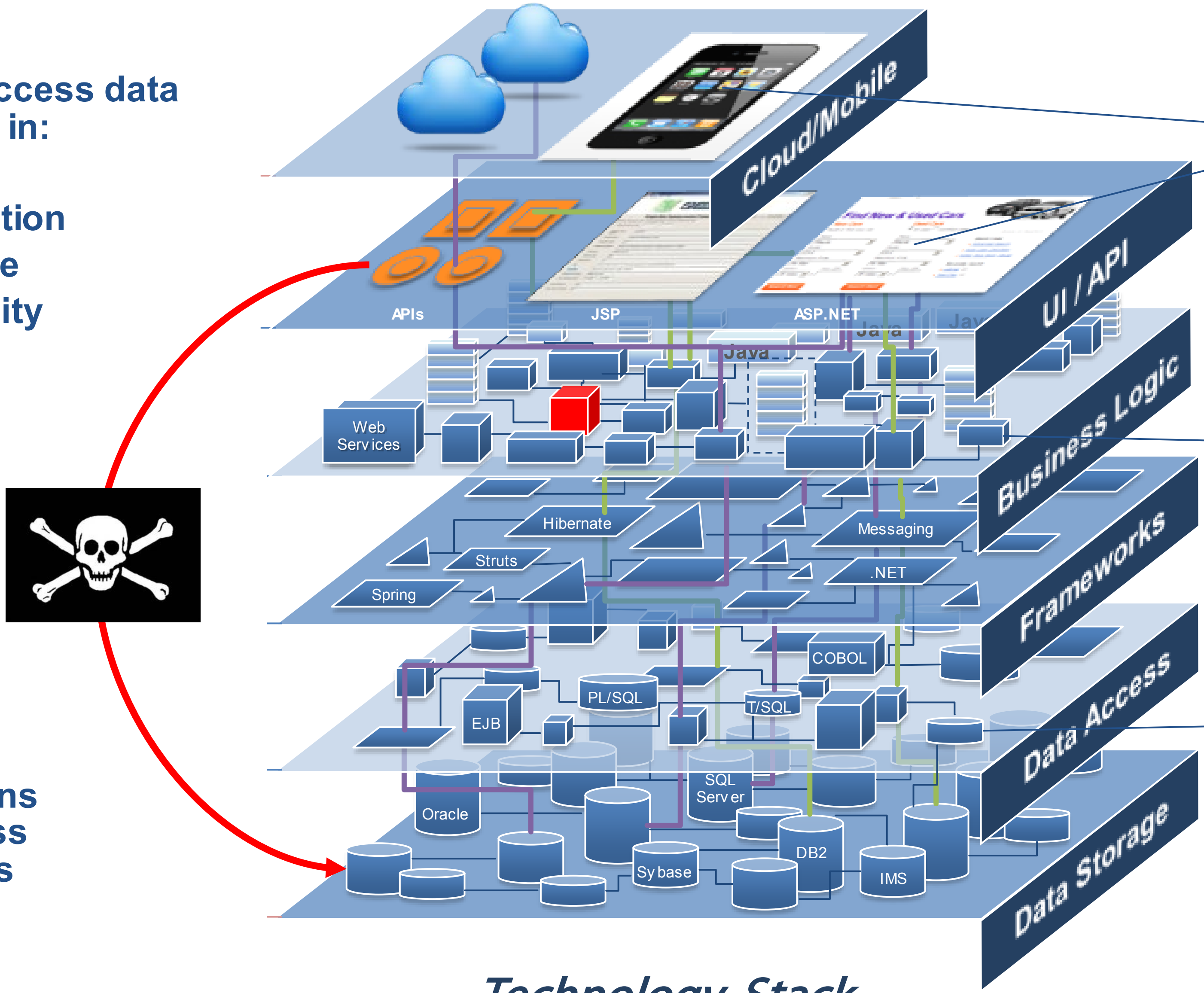
- Multiple languages
- Architectural compliance
- Risk propagation
- Application security
- Resiliency checks
- Transaction integrity
- Function points
- Integration quality
- Data access control
- SDK versioning
- Calibration across technologies
- IT organization level

CISQ
Consortium for IT Software Quality

Security Analysis Must Be System-Wide

Skipping layers to access data can cause problems in:

- Security
- Data corruption
- Performance
- Maintainability



Technology Stack

User entry

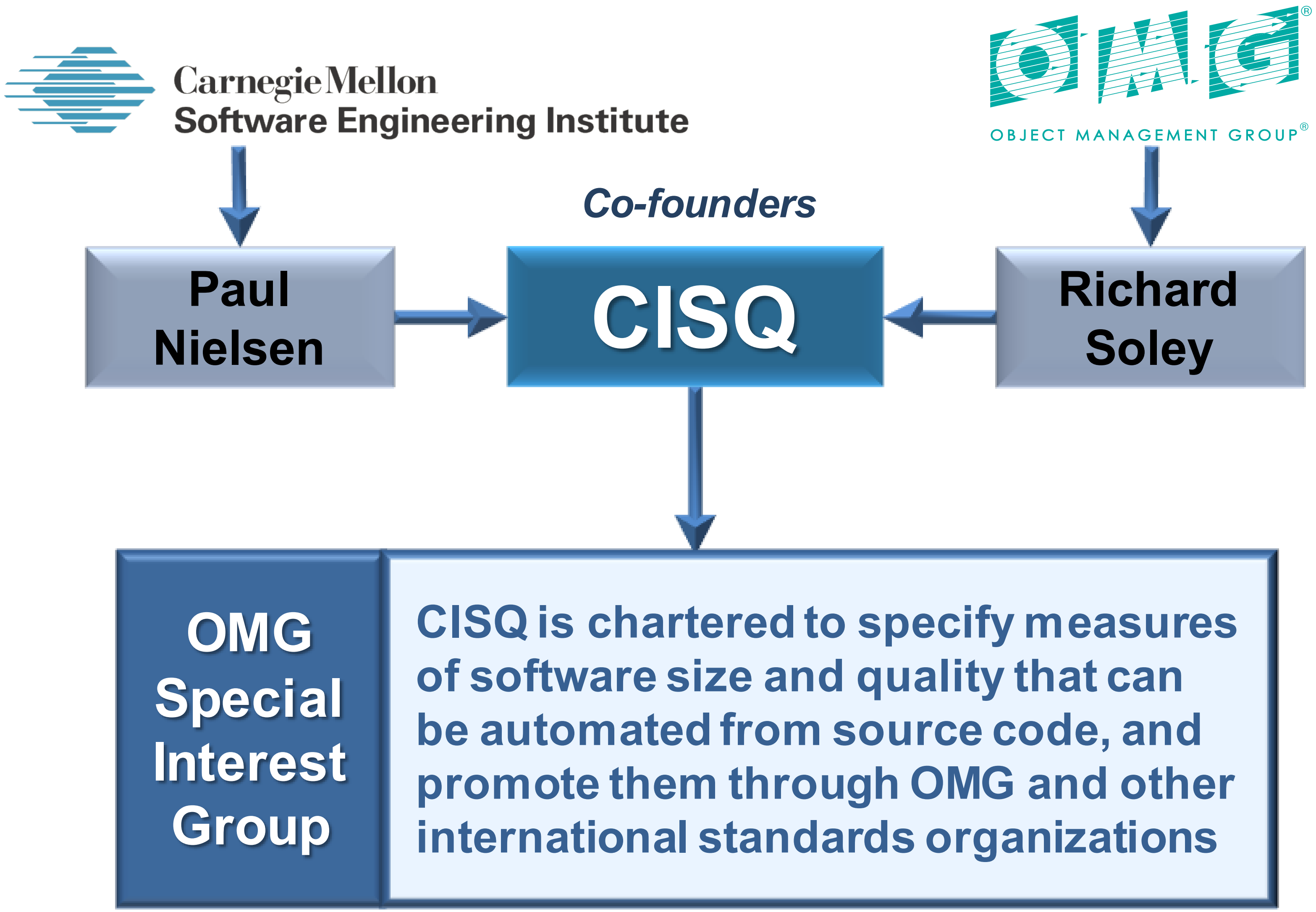
User & input authentication

Data access manager

Detection requires analyzing transactions and data flows across languages and layers

CISQ
Consortium for IT Software Quality

What Is CISQ ?



Carnegie Mellon
Software Engineering Institute

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

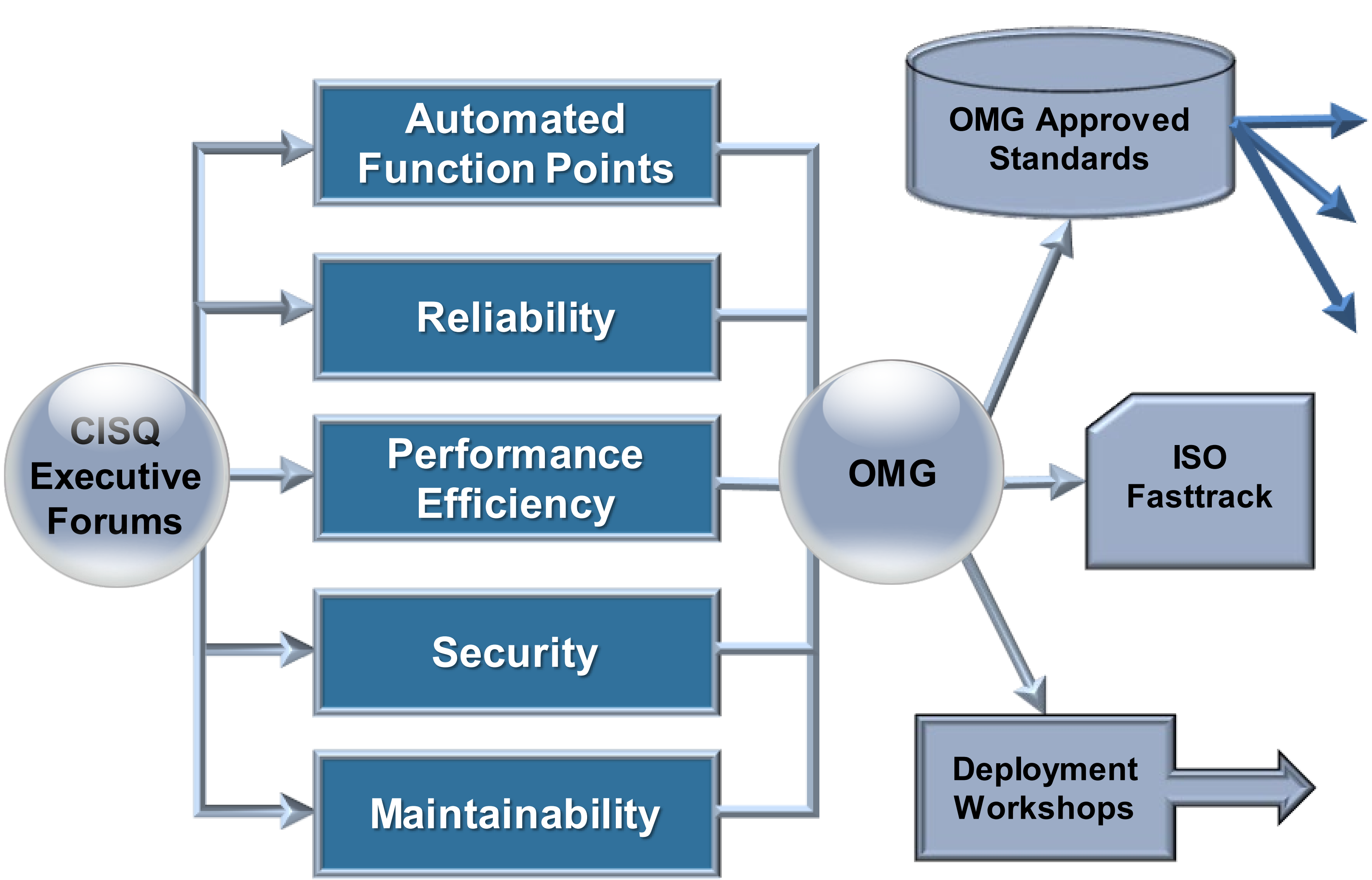
Cognizant
SYNOPSYS
Tech Mahindra
SHPI
CAST
CGI
NORTHROP GRUMMAN

CISQ Partners

Gartner
QuEST FORUM
FORRESTER
IAOP
ITAAC
AFCEA WASHINGTON, DC CHAPTER
TECHWELL
MAKING SOFTWARE BETTER

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

CISQ/OMG Standards Process



CISQ Executive Forums

Automated Function Points

Reliability

Performance Efficiency

Security

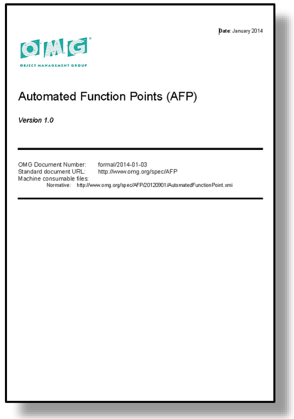
Maintainability

OMG

OMG Approved Standards

ISO Fasttrack

Deployment Workshops

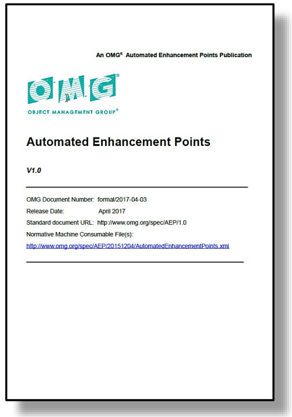


Date: January 2014

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



An OMG^R Automated Enhancement Points Publication

Automated Enhancement Points

V1.0

OMG Document Number: formal/2017-04-03
Release Date: April 2017
Standard document URL: http://www.omg.org/spec/AEP/1.0
Normative Machine Consumable File(s):
http://www.omg.org/spec/AEP/20151204/AutomatedEnhancementPoints.xmi

Date: January 2016

Automated Source Code Reliability Measure™ (ASCRM™)

V1.0

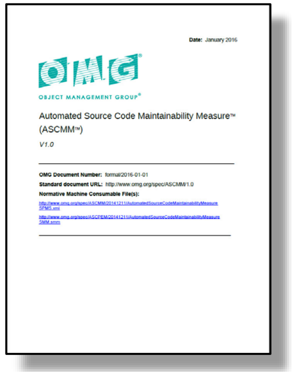
OMG Document Number: formal/2016-01-03
Standard document URL: http://www.omg.org/spec/ASCRM/1.0
Normative Machine Consumable File(s):
http://www.omg.org/spec/ASCRM/20141211/AutomatedSourceCodeReliabilityMeasureSPMS.xmi
http://www.omg.org/spec/ASCRM/20141111/AutomatedSourceCodeReliabilityMeasureSMM.smm

Date: January 2016

Automated Source Code Security Measure™ (ASCSM™)

V1.0

OMG Document Number: formal/2016-01-04
Standard document URL: http://www.omg.org/spec/ASCSM/1.0
Normative Machine Consumable File(s):
http://www.omg.org/spec/ASCSM/20150815/AutomatedSourceCodeSecurityMeasureSPMS.xmi
http://www.omg.org/spec/ASCSM/20150815/AutomatedSourceCodeSecurityMeasureSMM.xmi

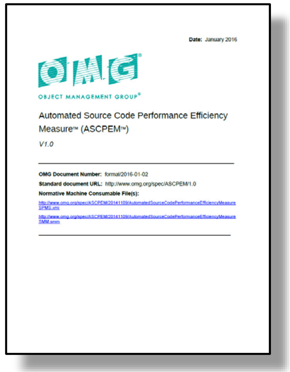


Date: January 2016

Automated Source Code Maintainability Measure™ (ASCMM™)

V1.0

OMG Document Number: formal/2016-01-01
Standard document URL: http://www.omg.org/spec/ASCMM/1.0
Normative Machine Consumable File(s):
http://www.omg.org/spec/ASCMM/20141211/AutomatedSourceCodeMaintainabilityMeasureSPMS.xmi
http://www.omg.org/spec/ASCPEM/20141211/AutomatedSourceCodeMaintainabilityMeasureSMM.smm



Date: January 2016

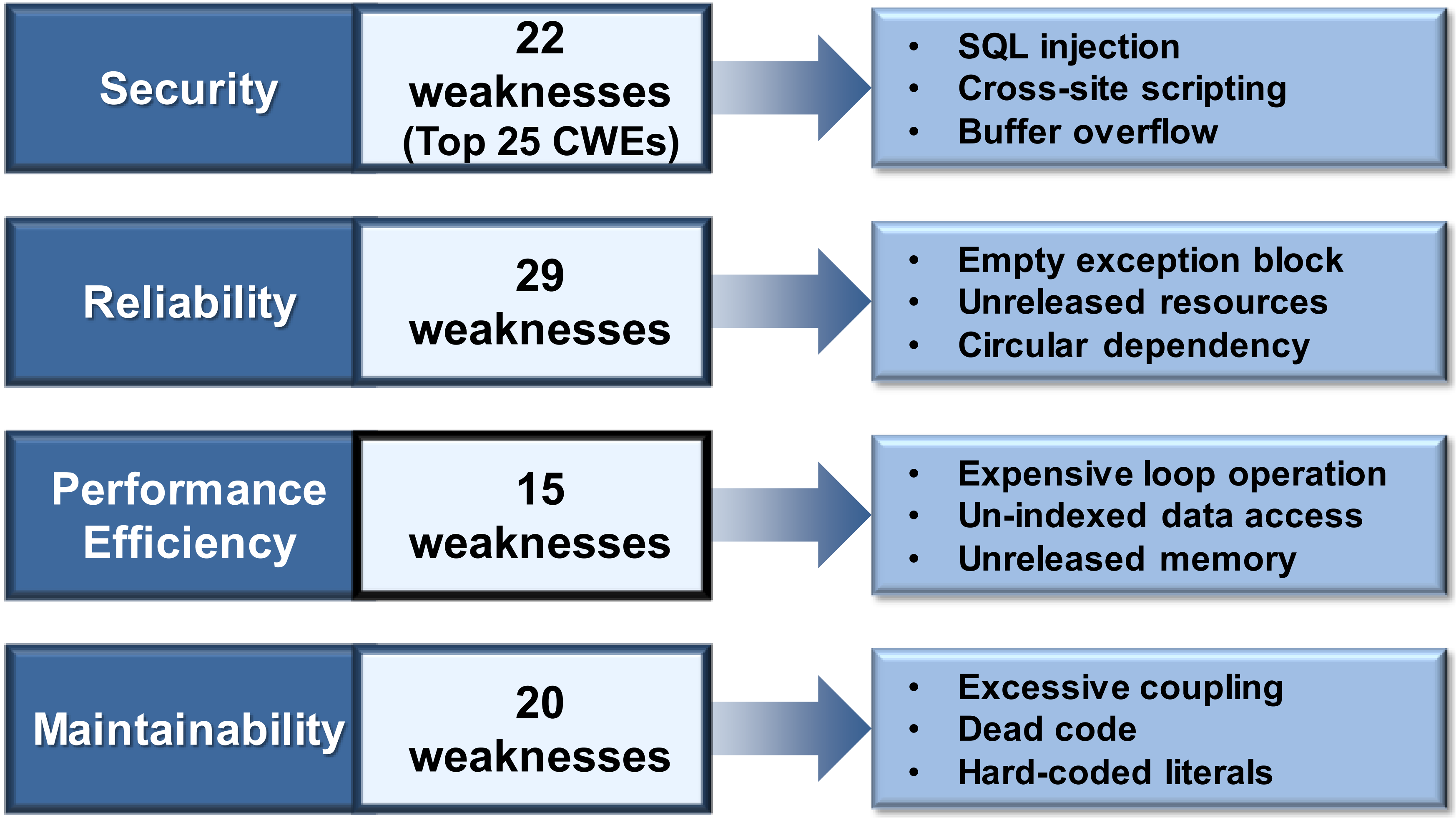
Automated Source Code Performance Efficiency Measure™ (ASCPEM™)

V1.0

OMG Document Number: formal/2016-01-02
Standard document URL: http://www.omg.org/spec/ASCPEM/1.0
Normative Machine Consumable File(s):
http://www.omg.org/spec/ASCPEM/20141109/AutomatedSourceCodePerformanceEfficiencyMeasureSPMS.xmi
http://www.omg.org/spec/ASCPEM/20141109/AutomatedSourceCodePerformanceEfficiencyMeasureSMM.smm

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.

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

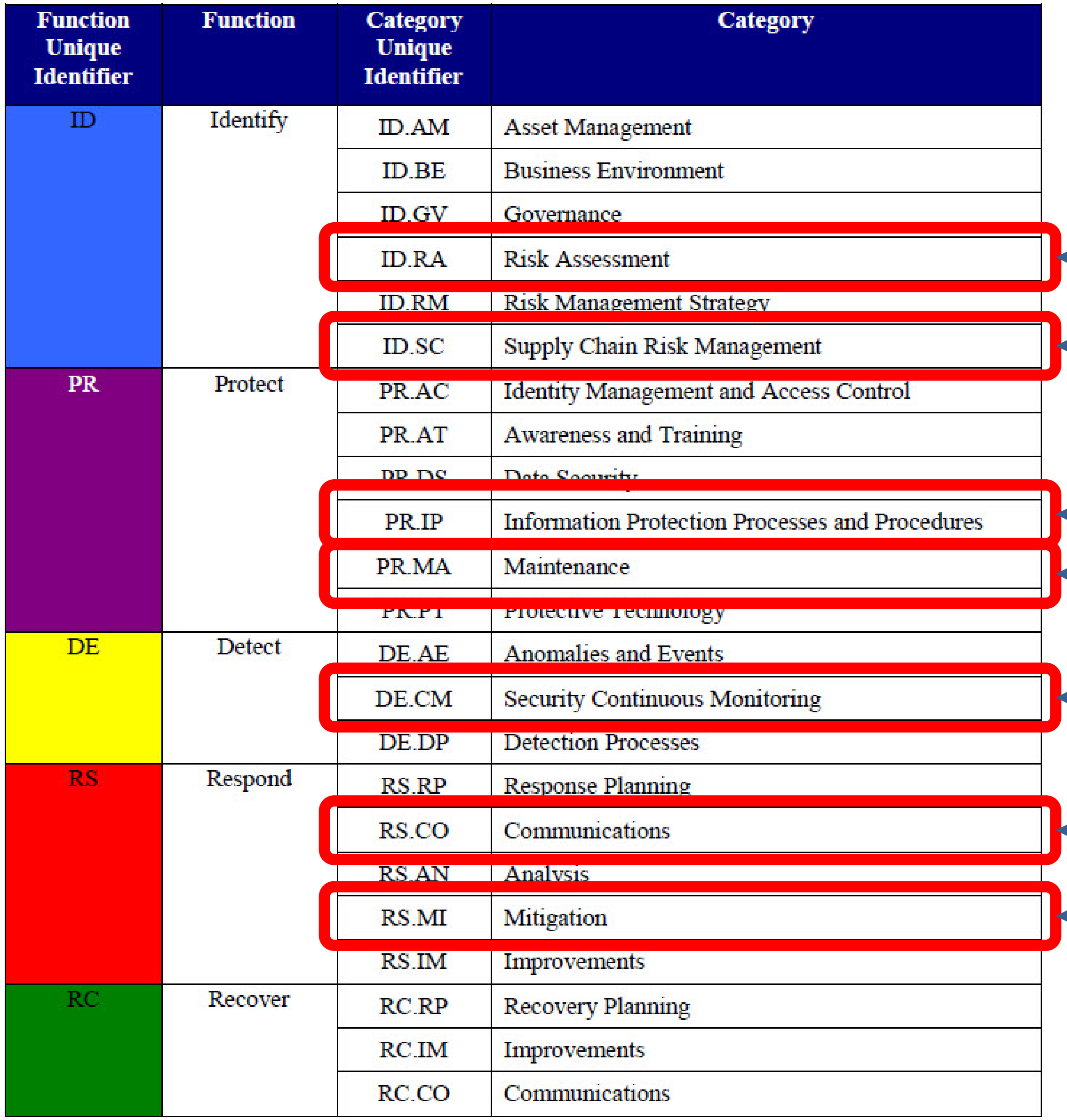
Common Weakness Enumeration
cwe.mitre.org

Update to CISQ measures:

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

CISQ
Consortium for IT Software Quality

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

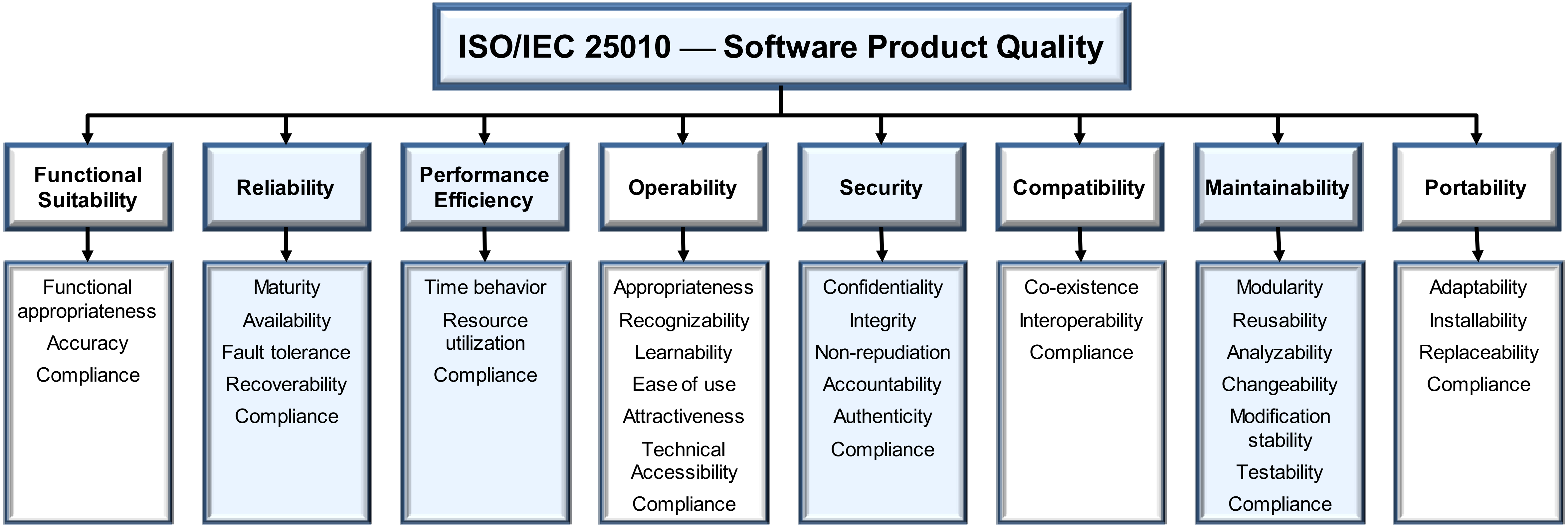
Security weaknesses are identified and mitigated

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

CISQ
Consortium for IT Software Quality

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: Functional appropriateness, Accuracy, Compliance

Reliability: Maturity, Availability, Fault tolerance, Recoverability, Compliance

Performance Efficiency: Time behavior, Resource utilization, Compliance

Operability: Appropriateness, Recognizability, Learnability, Ease of use, Attractiveness, Technical Accessibility, Compliance

Security: Confidentiality, Integrity, Non-repudiation, Accountability, Authenticity, Compliance

Compatibility: Co-existence, Interoperability, Compliance

Maintainability: Modularity, Reusability, Analyzability, Changeability, Modification stability, Testability, Compliance

Portability: Adaptability, Installability, Replaceability, Compliance

CISQ automated structural quality measures are highlighted in blue

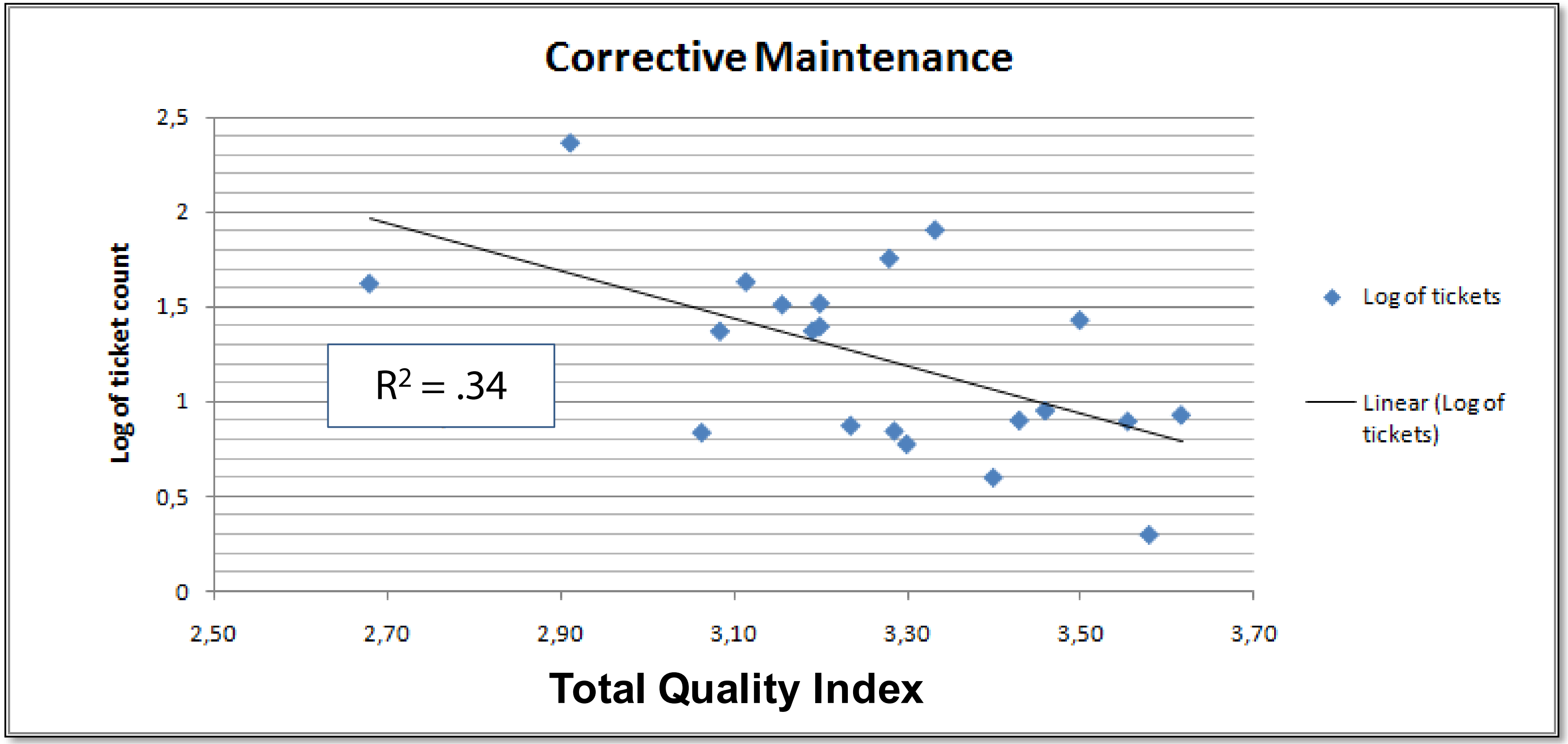
CISQ
Consortium for IT Software Quality

CISQ-like Measures Predict Incidents & Costs

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

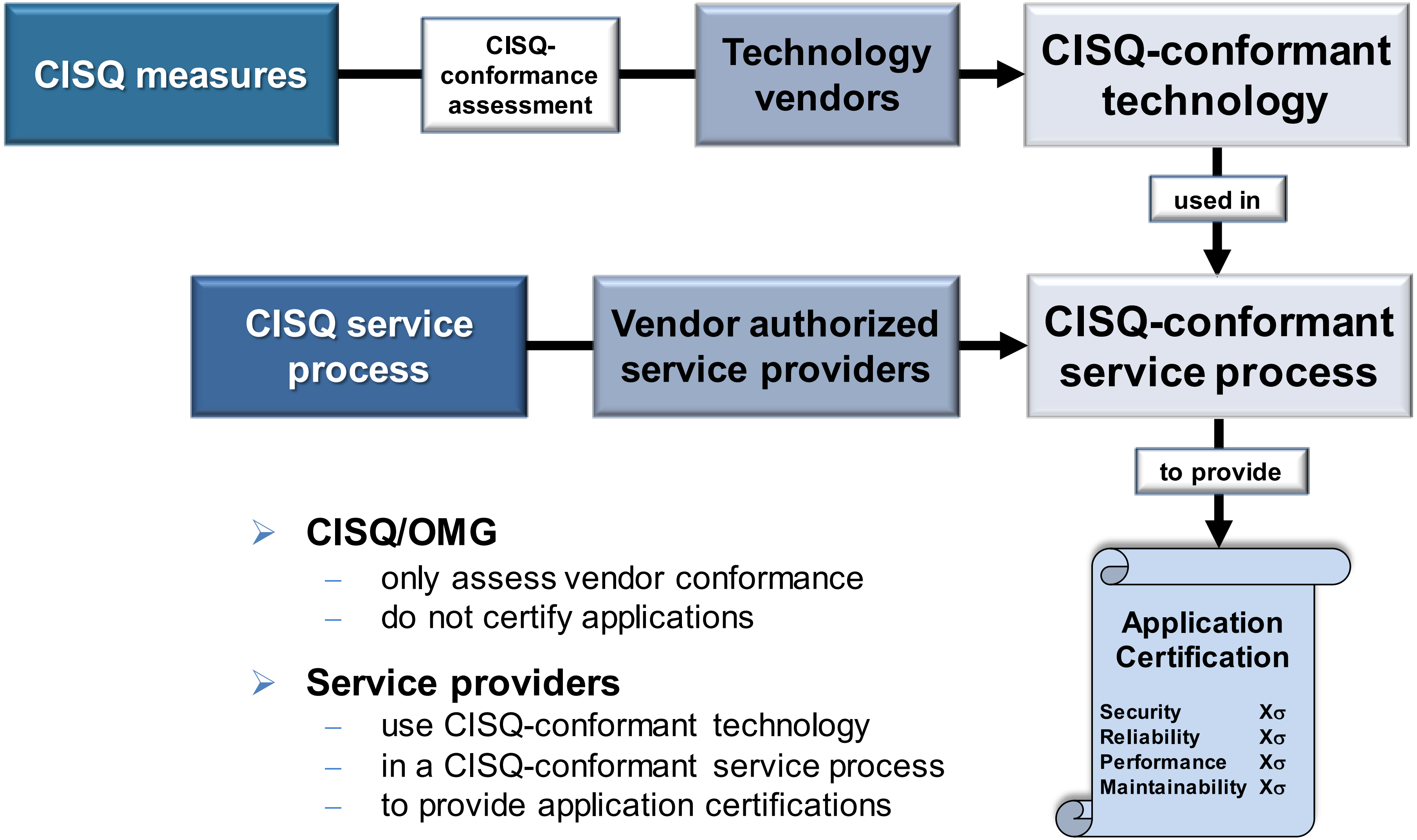
Increase in Total Quality Index of .24 decreased corrective maintenance effort 50%

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



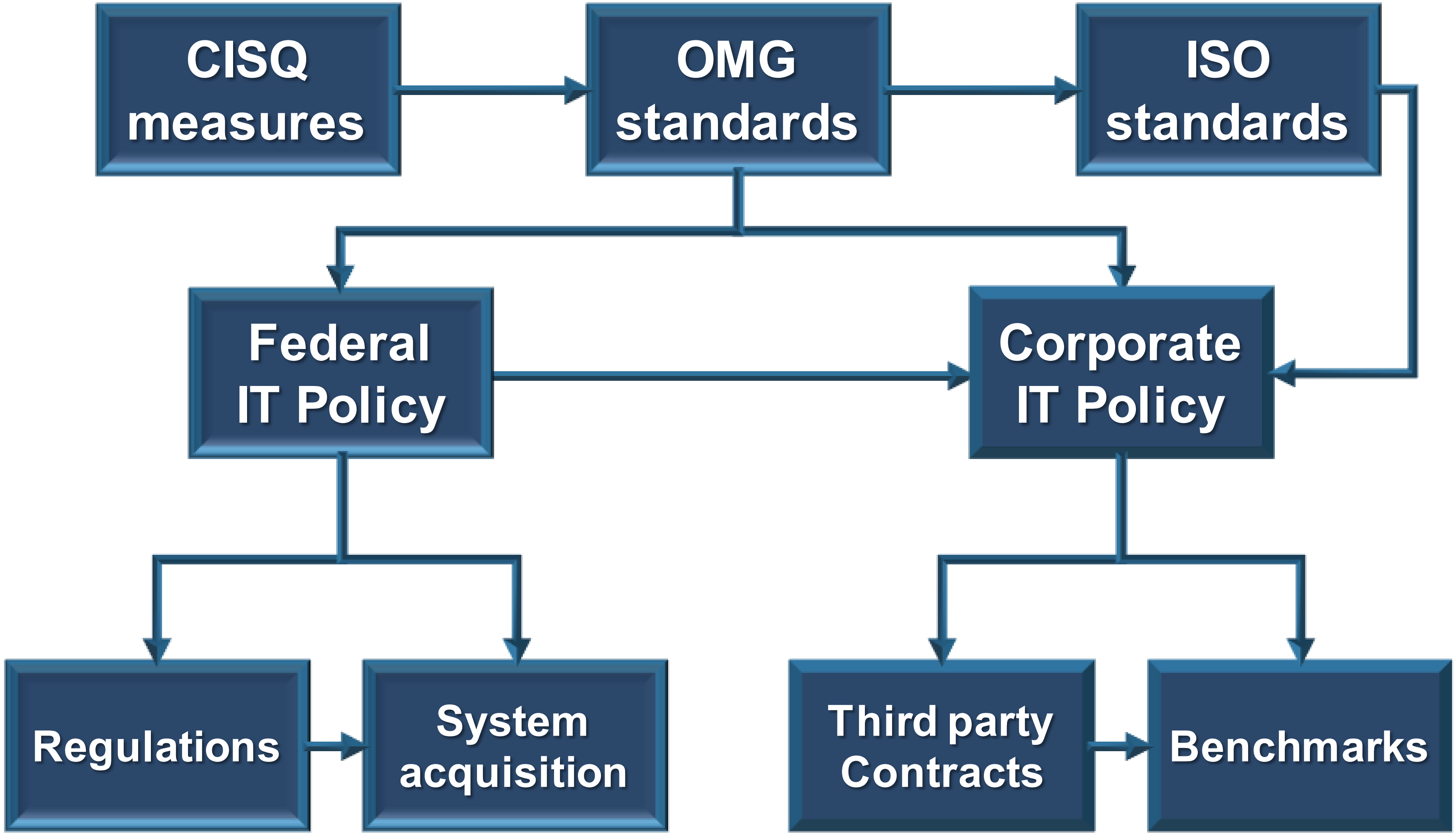
CISQ
Consortium for IT Software Quality

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

Deploying CISQ Measures



CISQ measures

OMG standards

ISO standards

Federal IT Policy

Corporate IT Policy

Regulations

System acquisition

Third party Contracts

Benchmarks

Sec. & Exch. Com.
State of Texas

US State Dept.
Gen. Serv. Admin.

1 — Engineering Discipline in Process and Product

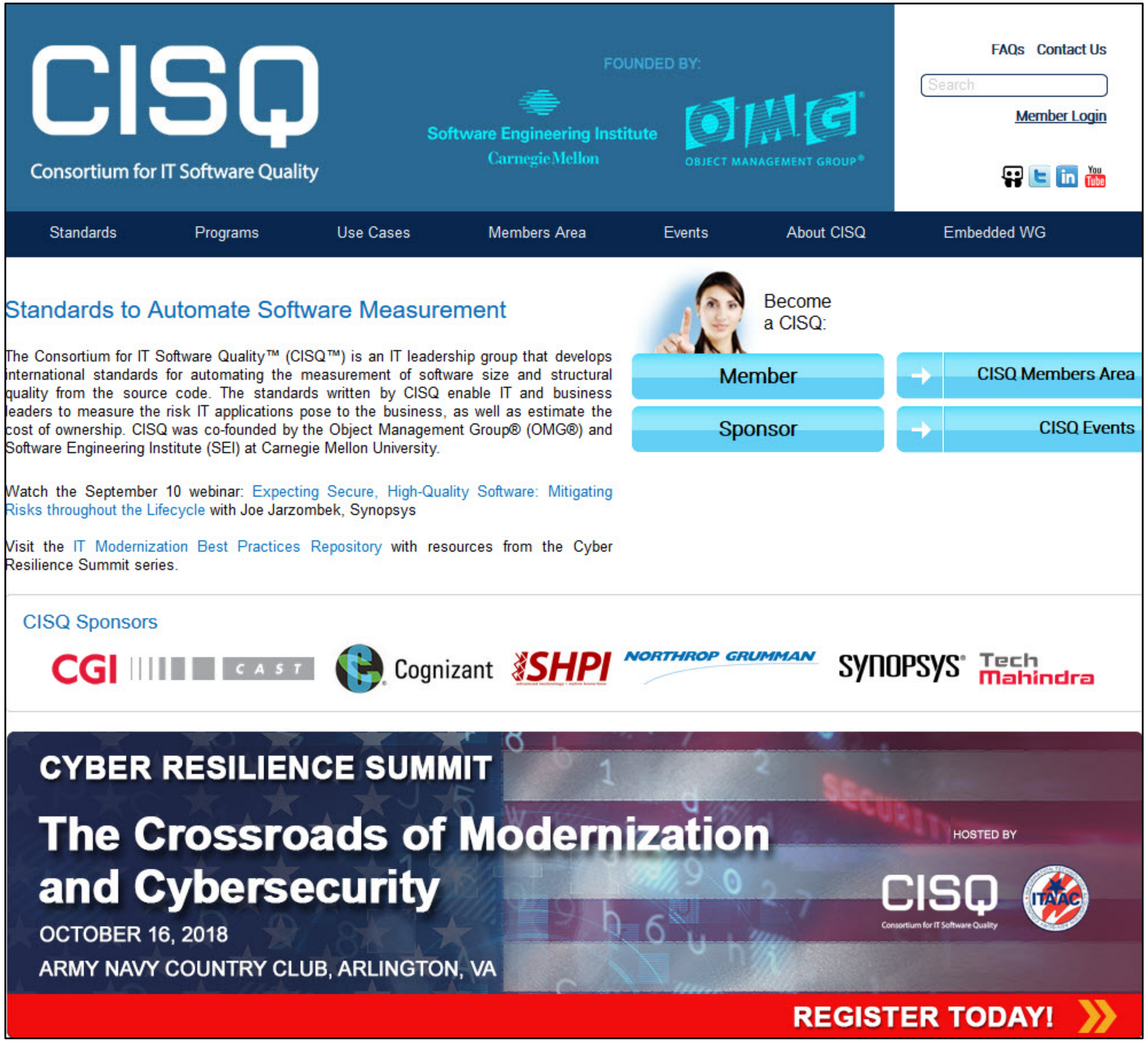
TRUSTWORTHY SYSTEMS MANIFESTO
We hold these truths to be self-evident
CISQ

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

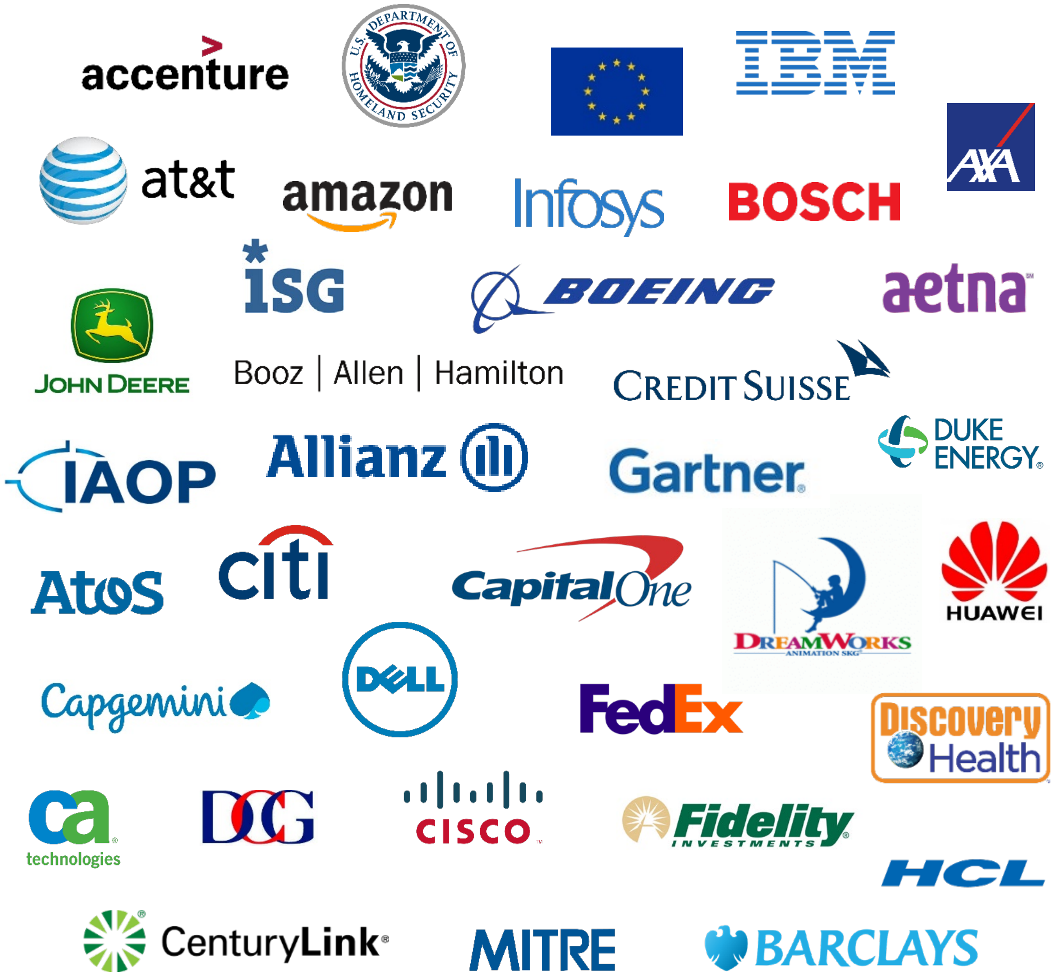
CYBER RESILIENCE SUMMIT

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
IAOP
Allianz
Gartner
Duke Energy
Atos
citi
Capital One
DreamWorks
HUAWEI
Capgemini
DELL
FedEx
Discovery Health
ca technologies
DCG
CISCO
Fidelity Investments
HCL
CenturyLink
MITRE
BARCLAYS