An Introduction to Automatable Standards for Software Measurement

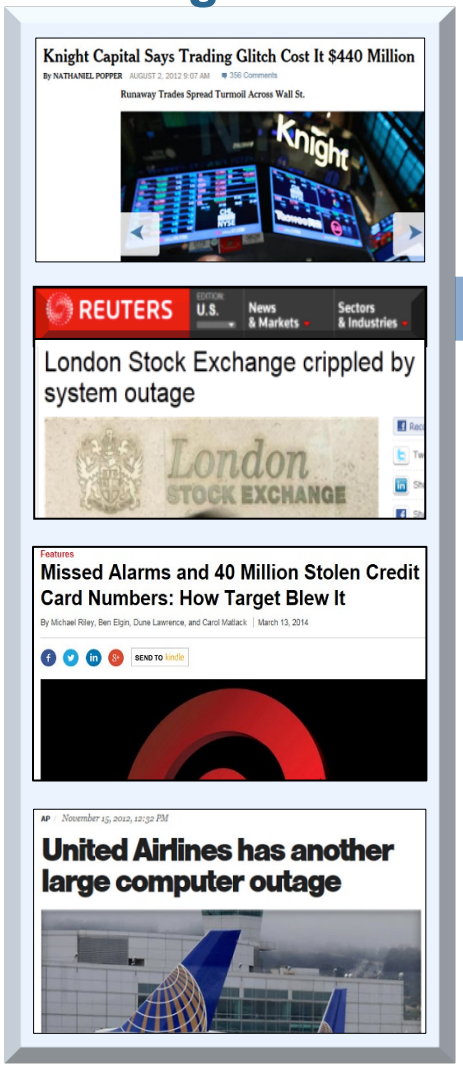
Dr. Bill Curtis
Executive Director

CISQ
Consortium for IT Software Quality

CISQ
Consortium for IT Software Quality

In the Era of 9-Digit Defects…

Nine Digit Defects



now affect

- Governor
- Texas Legislature
- DIR
- Agency Heads
- Agency CIOs

accountable for

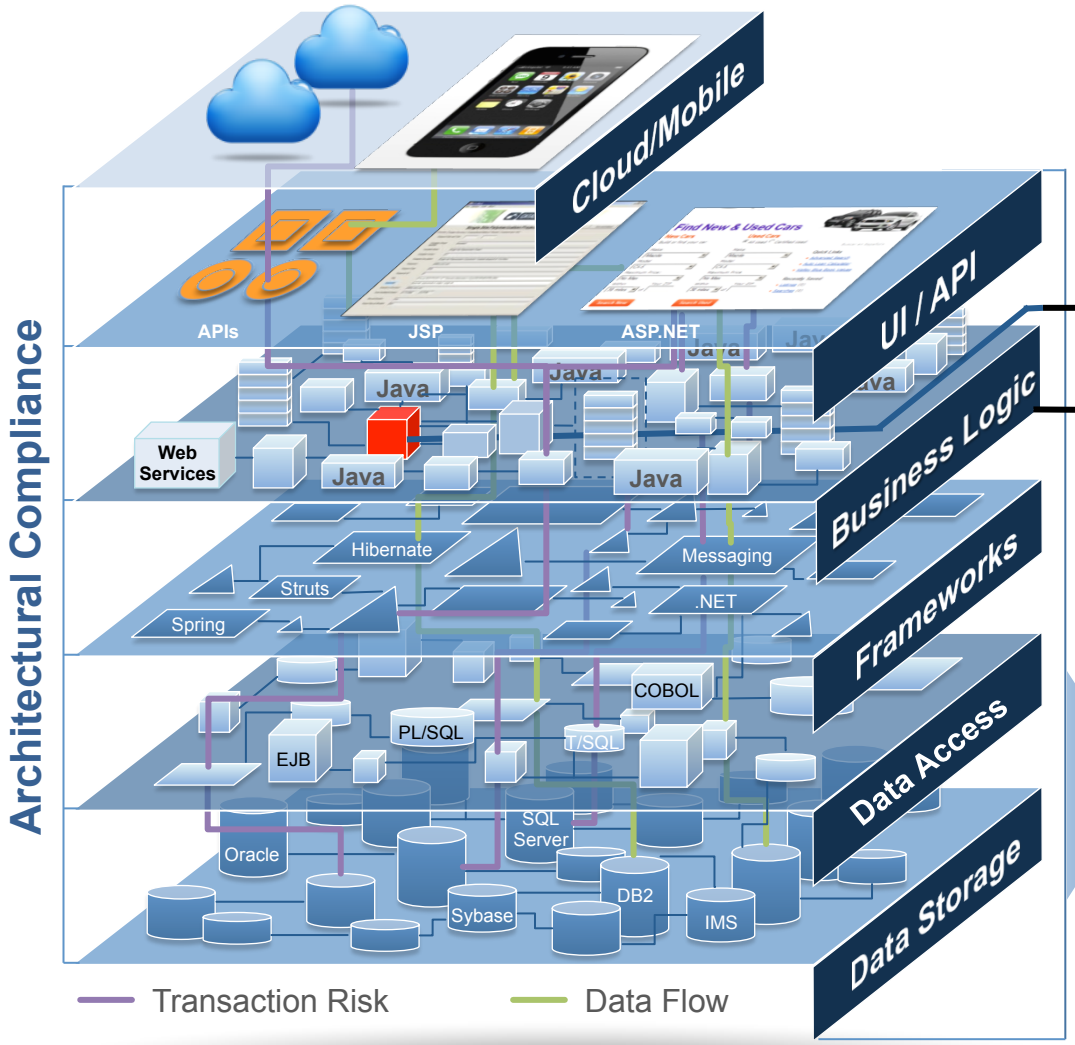
- Governance
- Risk management
- Risk measurement
- Taxpayer trust
- Customer UX

Need measures of progress and quality

© 2018. Consortium for IT Software Quality

CISQ
Consortium for IT Software Quality

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

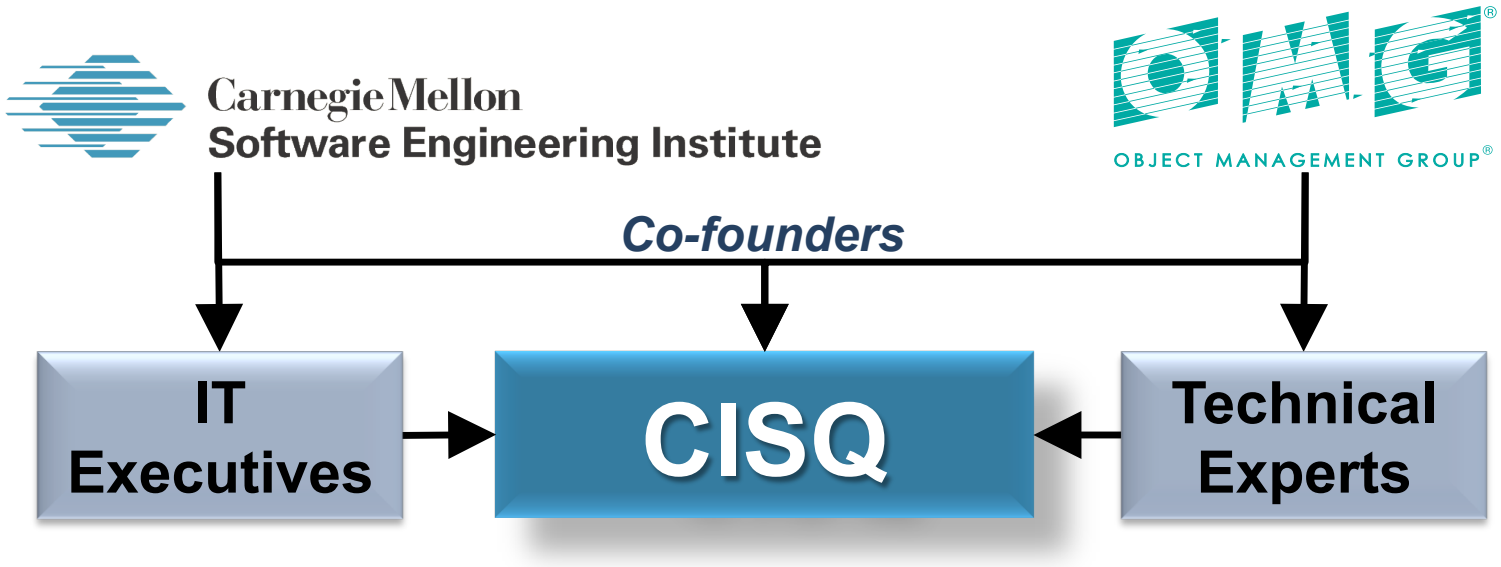
- Single language/technology layer
- Intra-technology architecture
- Intra-layer dependencies
- Inter-program invocation
- Security vulnerabilities
- Development team level

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

CISQ — 4th Generation Software Standards

CISQ
Consortium for IT Software Quality



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®

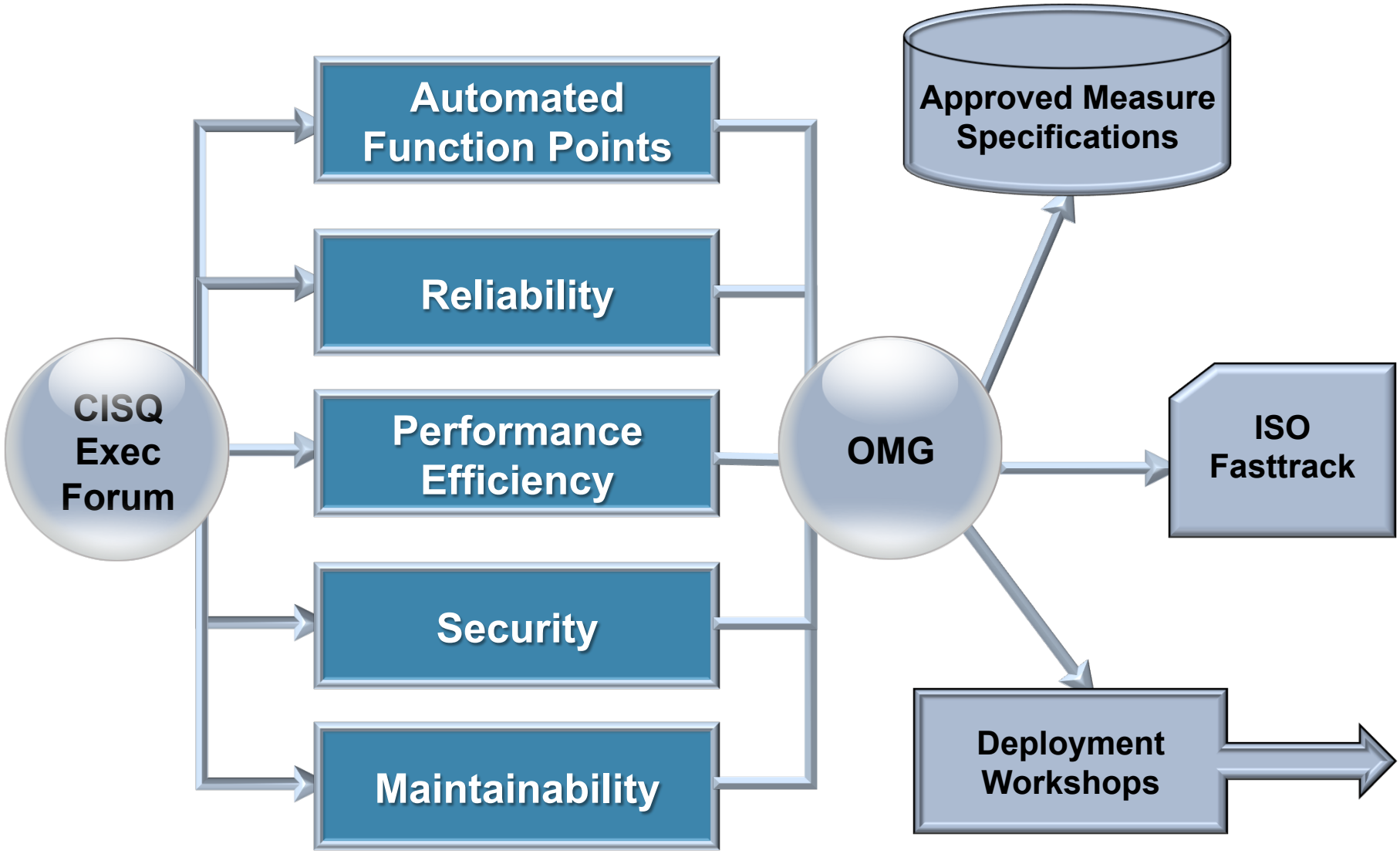
CISQ Sponsors

SYNOPSYS®
Cognizant
SHPI
advanced technology • native know-how
Tech Mahindra
CAST
CGI
NORTHROP GRUMMAN

Copyright © 2018 CISQ. All rights reserved.

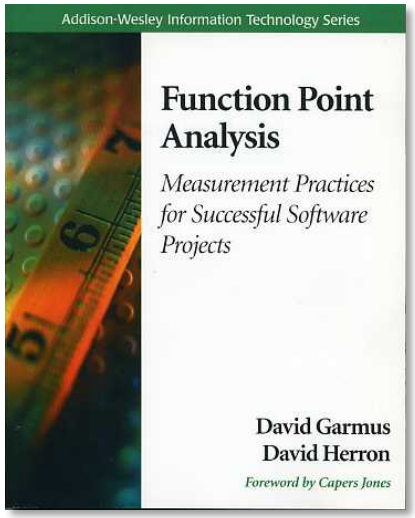
CISQ
Consortium for IT Software Quality

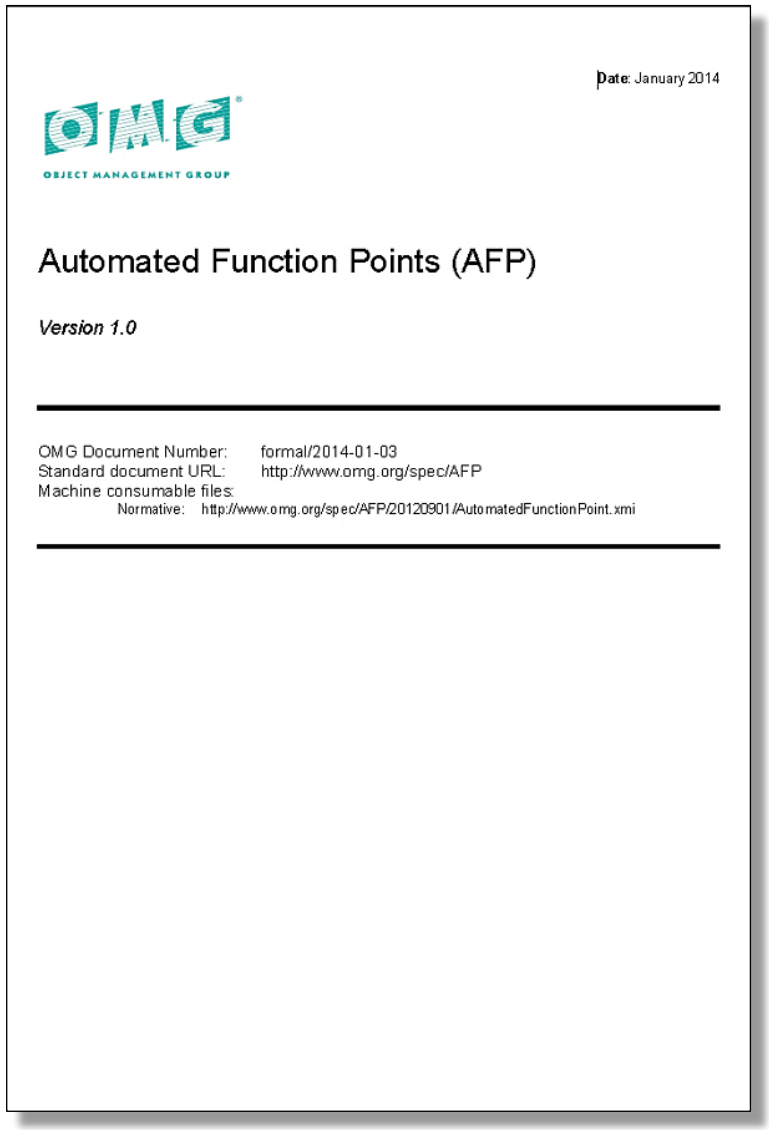
CISQ/OMG Standards Process



Automated Size Measurement

- **Mirrors IFPUG counting guidelines, but automatable**
- **Specification developed by international team led by David Herron of David Consulting Group**
- **Submitted thru OMG's fasttrack as ISO 19515, currently under review**





Date: January 2014

OBJECT MANAGEMENT GROUP

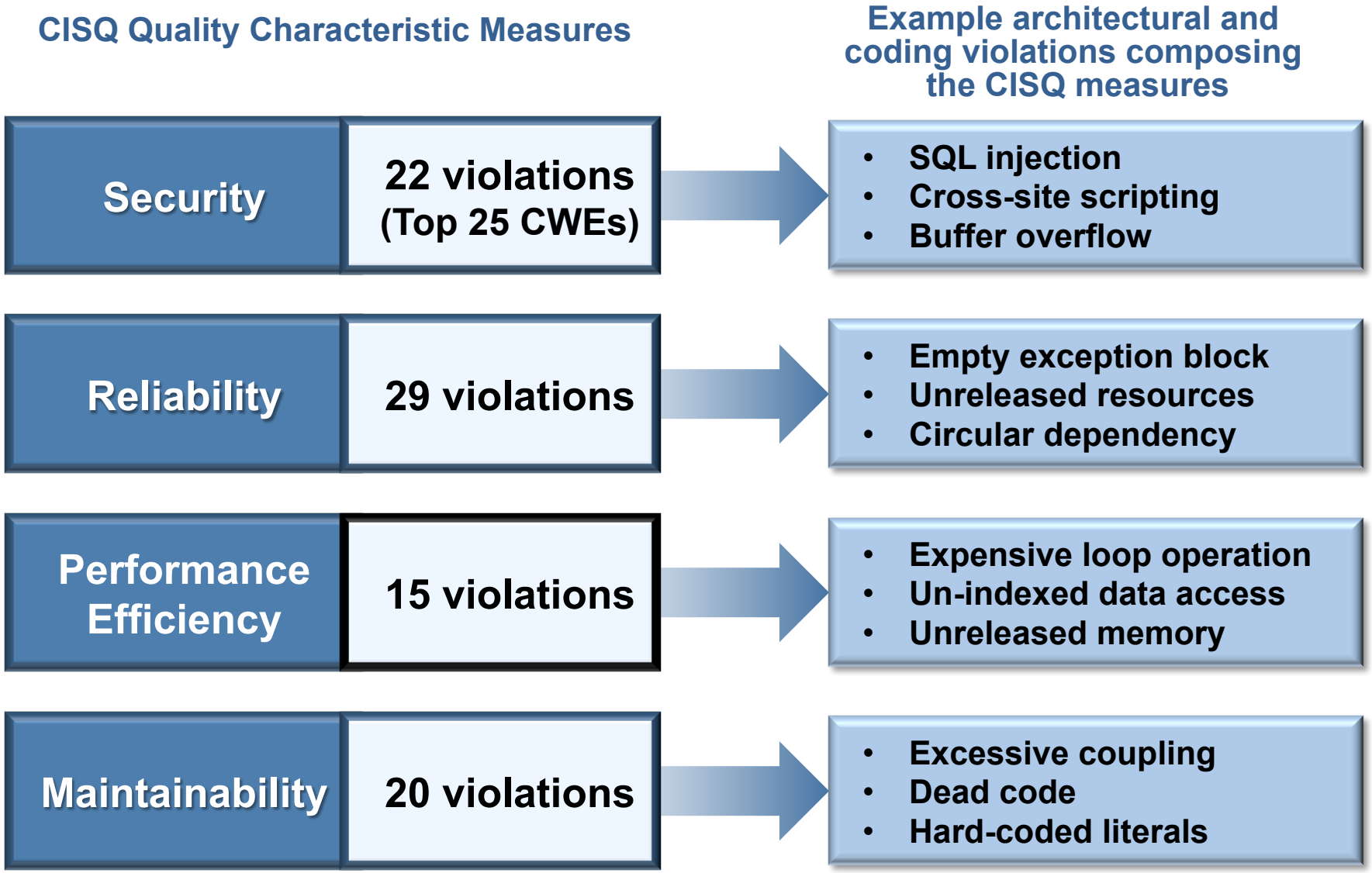
Automated Function Points (AFP)

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

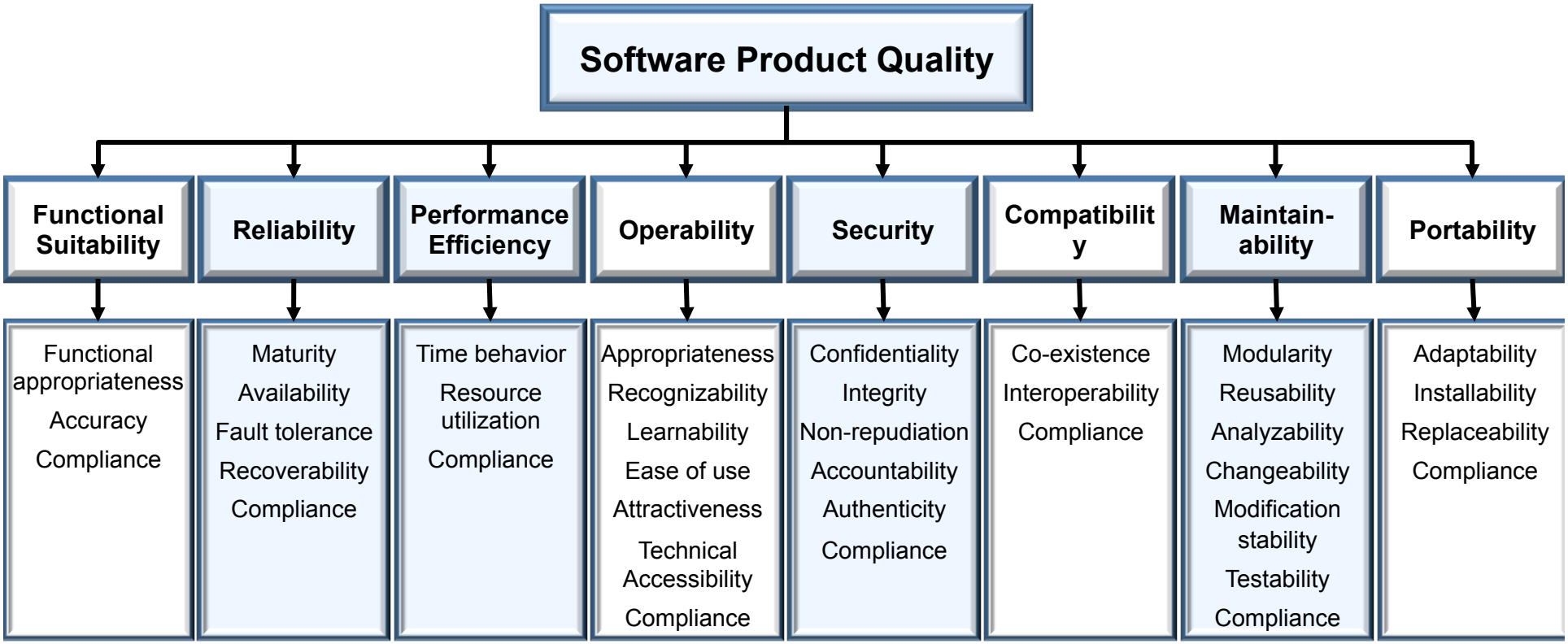
CISQ Quality Characteristic Measures

Consortium for IT Software Quality



CISQ Conforms/Supplements ISO 25000 series

- **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

22 CWEs Form the CISQ 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 Resou
- 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')

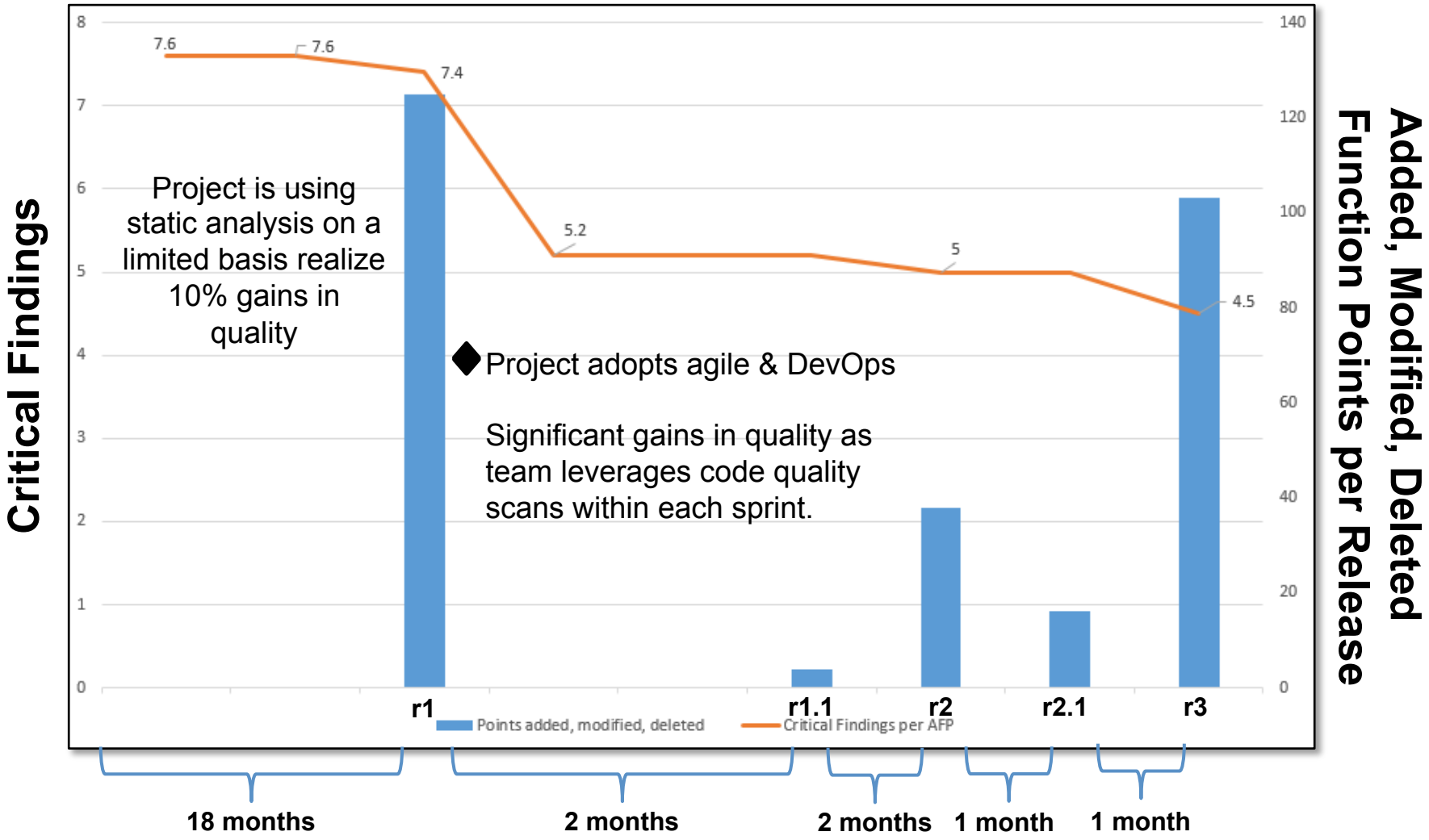
Robert Martin
MITRE

CWE

Common Weakness Enumeration
cwe.mitre.org

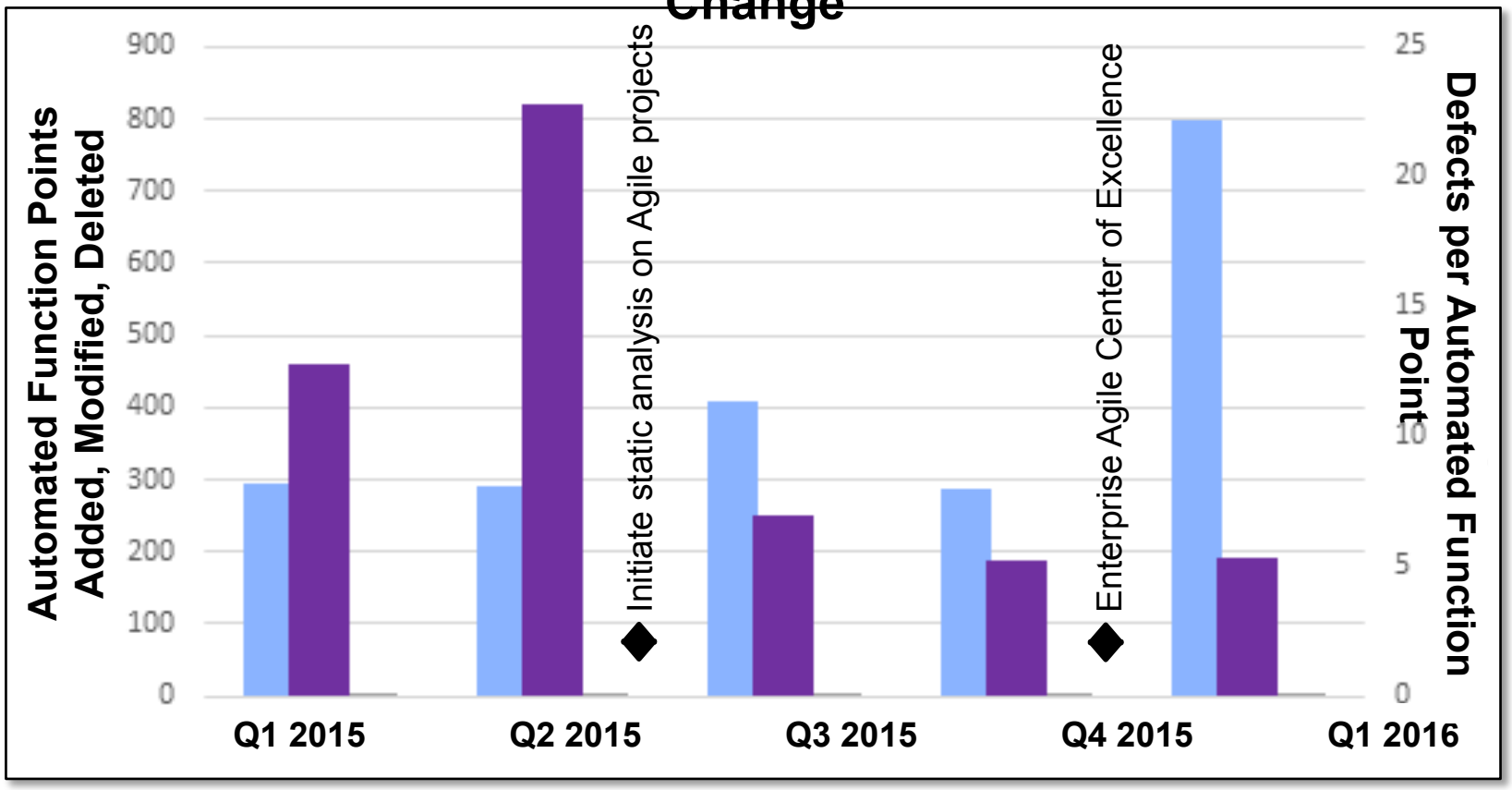
CISQ
Consortium for IT Software Quality

Fannie Mae's Agile Transformation — 1



Fannie Mae's Agile Transformation — 2

Improvement of Quality with Simultaneous Increase in Change



CISQ
Consortium for IT Software Quality

CISQ Measures in System Acquisition

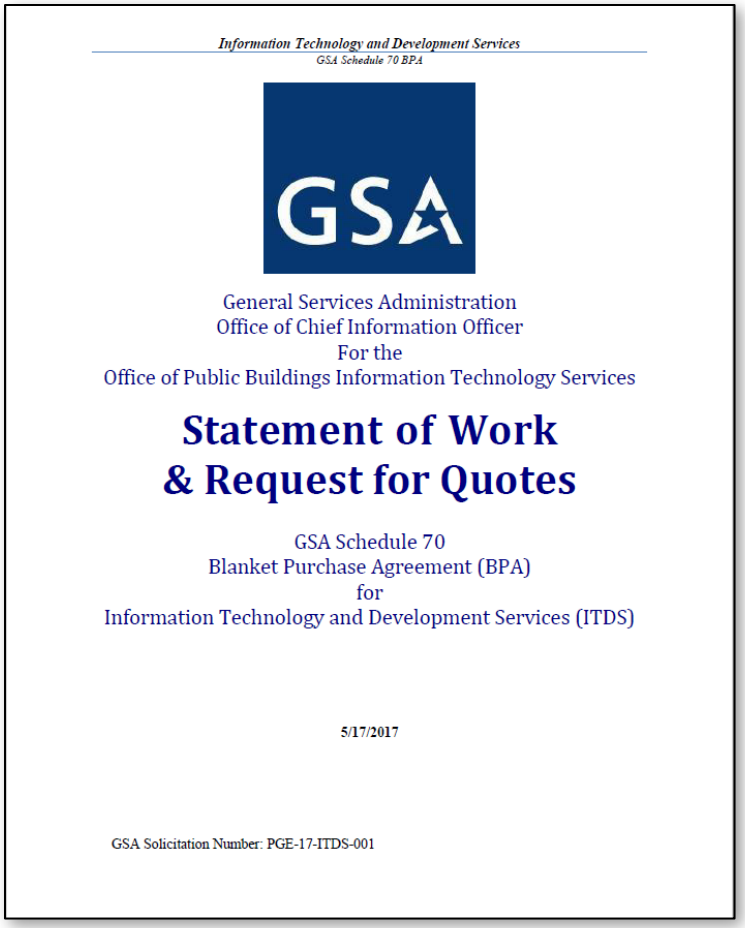
RFP — Include quality requirements and measures in project definition

SLA — Create quality targets using CISQ measures to set thresholds

SOW — Include software measurement and analysis as periodic project tasks

UAT — Measure against quality targets during acceptance testing

CISQ Referenced by GSA



Information Technology and Development Services
GSA Schedule 70 BPA

GSA

General Services Administration
Office of Chief Information Officer
For the
Office of Public Buildings Information Technology Services

Statement of Work
& Request for Quotes

GSA Schedule 70
Blanket Purchase Agreement (BPA)
for
Information Technology and Development Services (ITDS)

5/17/2017

GSA Solicitation Number: PGE-17-ITDS-001

CISQ was referenced by the U.S. General Services Administration (GSA), in an Information Technology (IT) statement of work from the Office of the CIO in the Office of Public Buildings.

Page 21, section 5.9: Schedule 70 Blank Purchase Agreement for IT and Development Services…

"PB-ITS (Project Based IT Services) is seeking to establish code quality standards for its existing code base, as well as new development tasks. As an emerging standard, PB-ITS references the Consortium for IT Software Quality (CISQ) for guidance on how to measure, evaluate and improve software."

Sample Service Level 'At Risk' Matrix

CISQ Consortium for IT Software Quality

At Risk Amount and Allocation of Risk

Total Billing Per Release :	$1,000,000
Total At Risk Amount (10% of Bill) :	$100,000
Total Risk Pooler:	100%

10% is for example

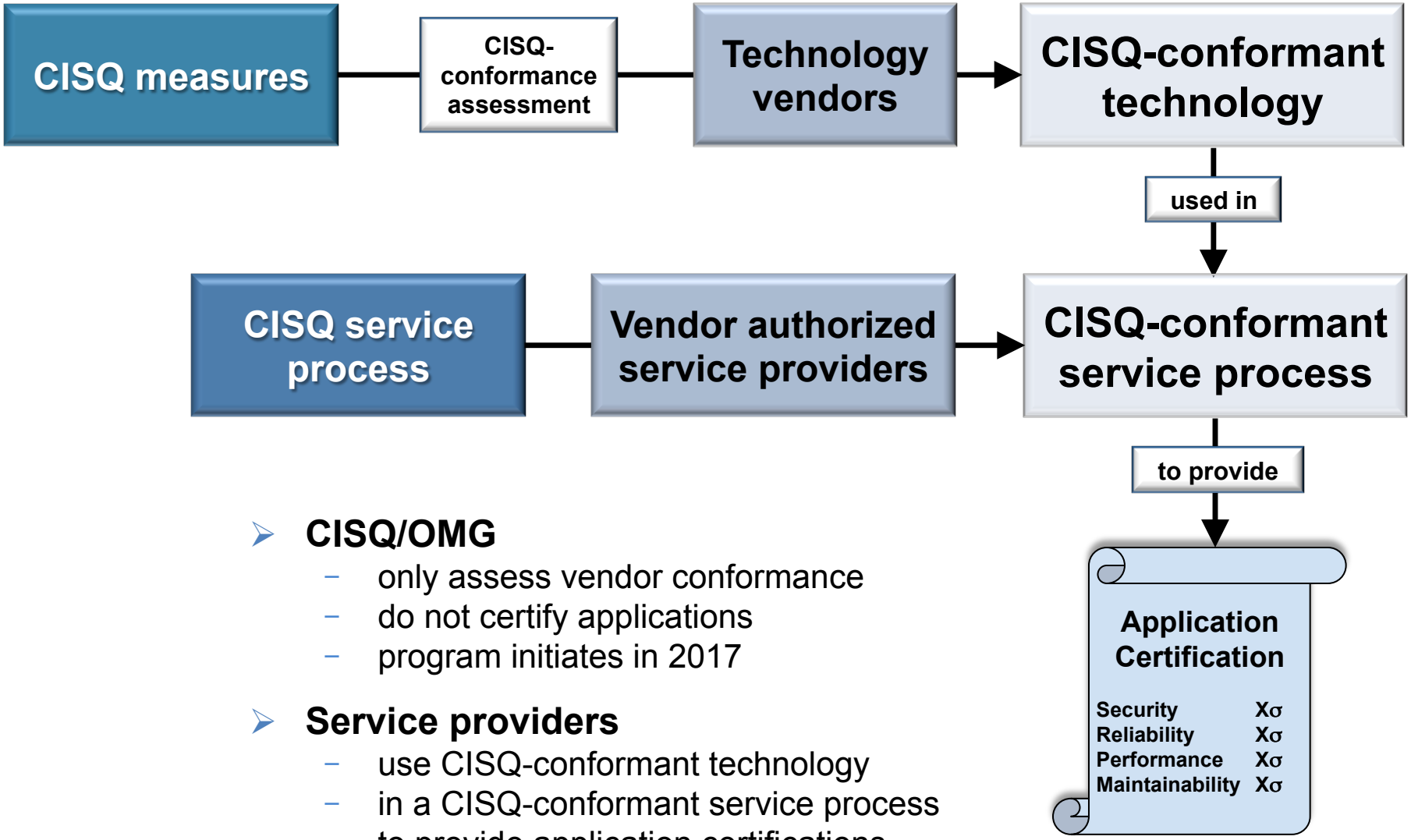
Application Name	Tier 1 Metrics (Critical Service Levels)	At Risk Multiplier	Risk Allocation	At Risk Amount
OMS			30%	
	Security Findings	50%		$15,000
	Reliability Findings	30%		$9,000
	Application Pain Violations	20%		$6,000
		100%		$30,000
CRM			10%	
	Security Findings	30%		$3,000
	Reliability Findings	30%		$3,000
	Application Pain Violations	40%		$4,000
		100%		$10,000
AMSS			20%	
	Security Findings	50%		$10,000
	Reliability Findings	30%		$6,000
	Application Pain Violations	20%		$4,000
		100%		$20,000
SDP			20%	
	Security Findings	50%		$10,000
	Reliability Findings	30%		$6,000
	Application Pain Violations	20%		$4,000
		100%		$20,000
Enabler			20%	
	Security Findings	50%		$10,000
	Reliability Findings	30%		$6,000
	Application Pain Violations	20%		$4,000
		100%		$20,000

Amount service provider has at risk in this Service Level is

30% * 50% * $100K = $15,000

- Any time there is a default, the at-risk amount will be applied
- Incentive is given to the at risk amount if Service Provider exceeds the Expected Service Level by 5% of the delta between the then current Expected and Perfection
- Credits / Incentives are settled at the Annual Reset

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

CISQ Home — www.it-cisq.org