

How Can VMOs Ensure Vendor-Supplied Software is Trustworthy?

IAOP Webinar
February 6, 2019

Dr. Bill Curtis
Executive Director, CISQ



International Standards for
Automating Software Size and
Structural Quality Measurement

Consortium for IT Software Quality



75%

Of vendors' developers have less than 3 years experience

10x

Difference between experienced and novice developer

\$25↑

Hourly rate card of outsourced developers continually rises

30+%

Annual turnover creates constant learning curve destroying benefits of labor arbitrage

Projected business value

LOWEST BUSINESS VALUE
HIGHEST COST PRESSURE

Input-based contract

- Time & materials
- Fixed capacity
- Low incentive

Output-based contract

- Size (Function Points)
- Incidents, Tickets
- Velocity, Delivery rate
- Quality, Delivered defects

HIGHEST BUSINESS VALUE
LOWEST COST PRESSURE

Outcome-based contract

- Service delivered
- Impact on business
- Satisfaction



**OUTCOME-BASED
CONTRACTS ARE
GROWING RAPIDLY**

50%

shifting to
outcome-based
contracts

57%

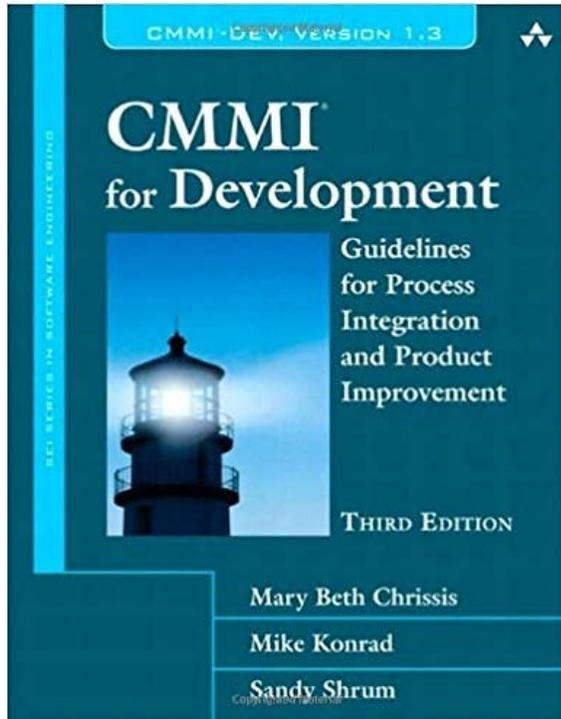
of CIOs and CTOs find
outcome-based
contracts most effective

Source: Deloitte 2014 Global Outsourcing and Insourcing Survey

	2015	2020
Delivery Model	Offshore: 80% Onsite: 20%	Offshore: 60% Onsite, Nearshore: 40%

Source: ISG December 2016 The Three Waves in the Evolution of the Engineering Services Outsourcing Industry

Process focus

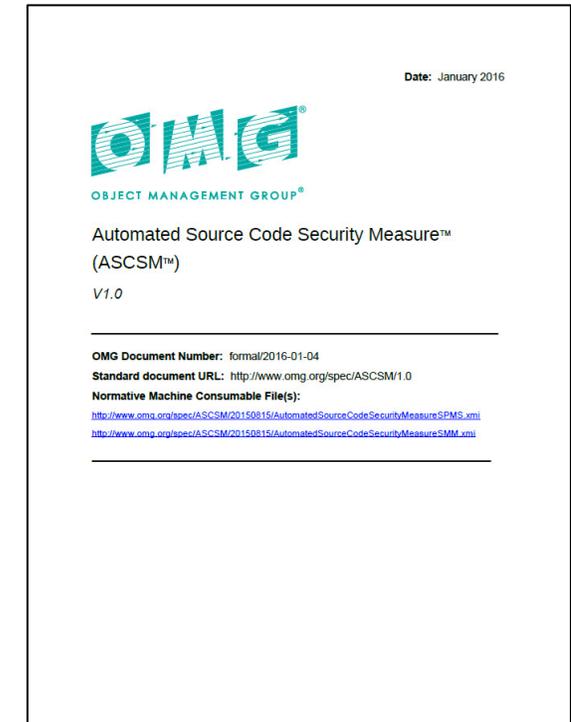


Contributes to, but does not measure or guarantee product quality

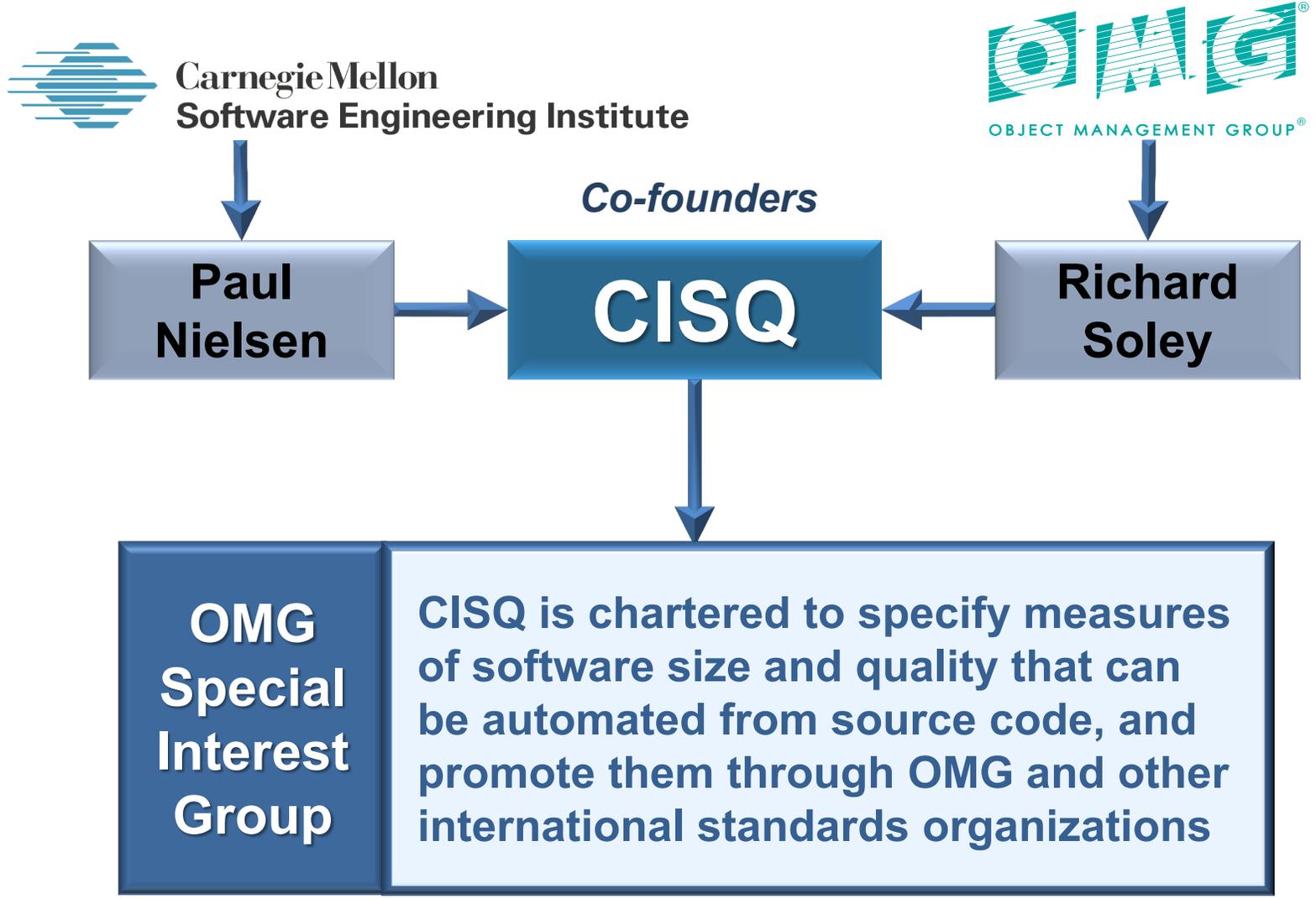
Must be supplemented by software product measurement before and during acceptance



Product focus



CISQ Measures assess the structural quality of the delivered software product

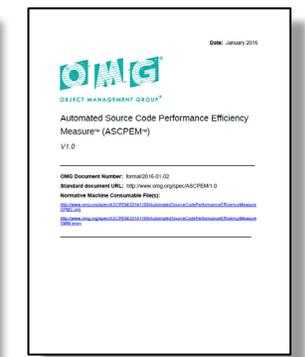
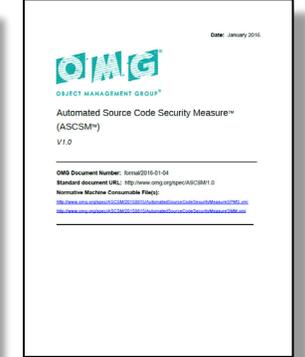
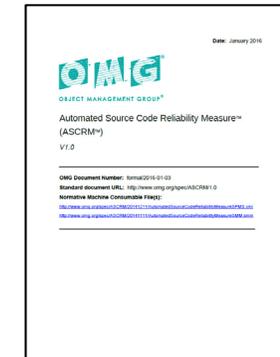
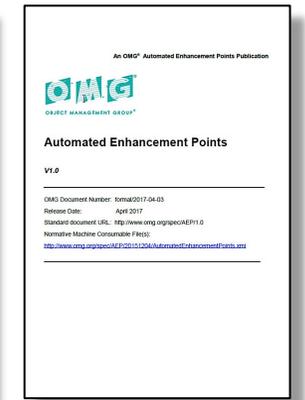
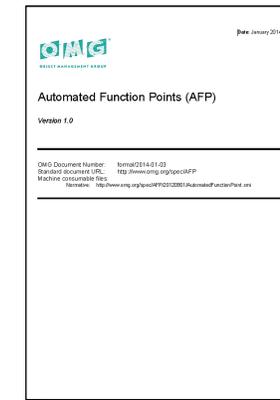
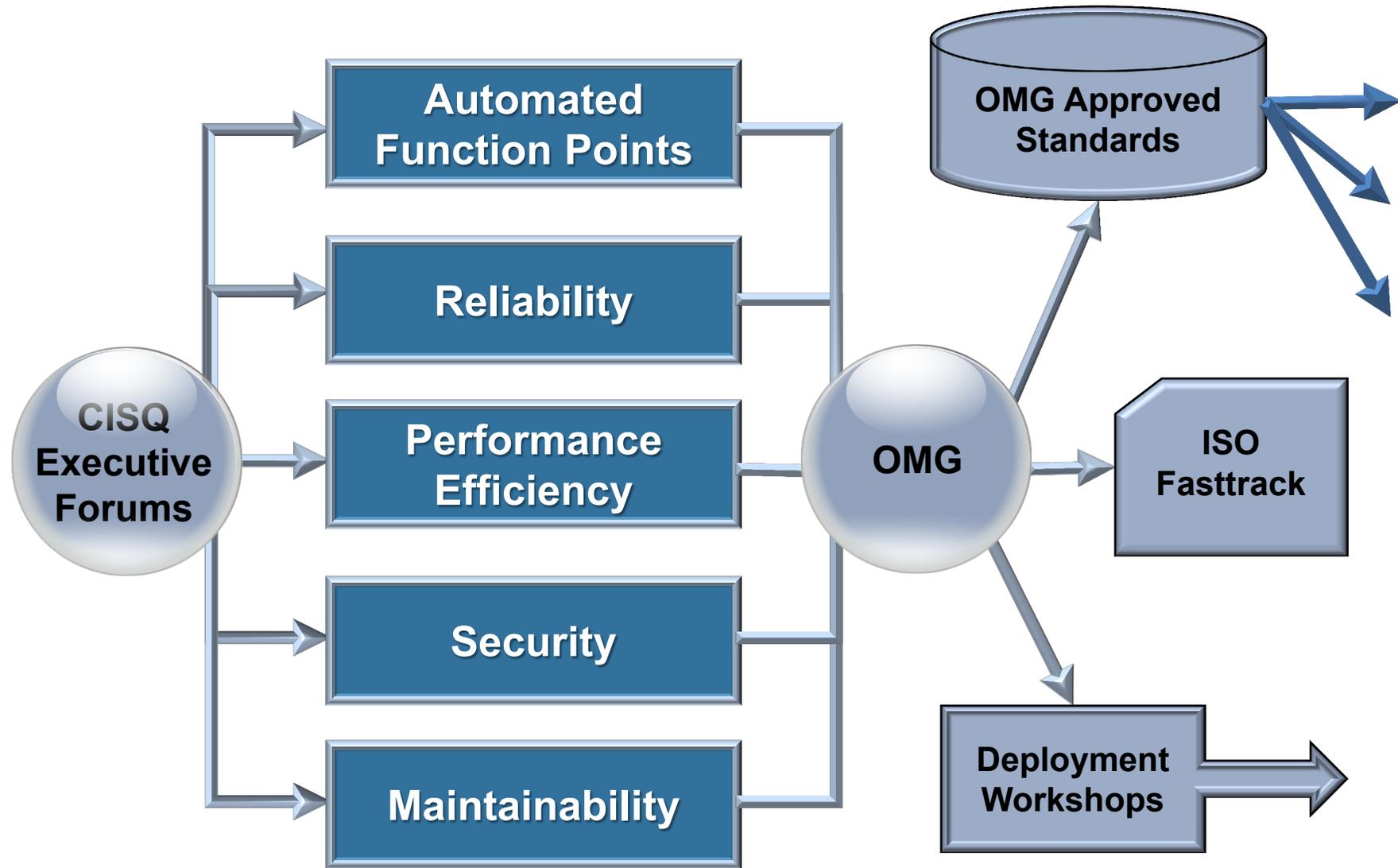


CISQ Sponsors

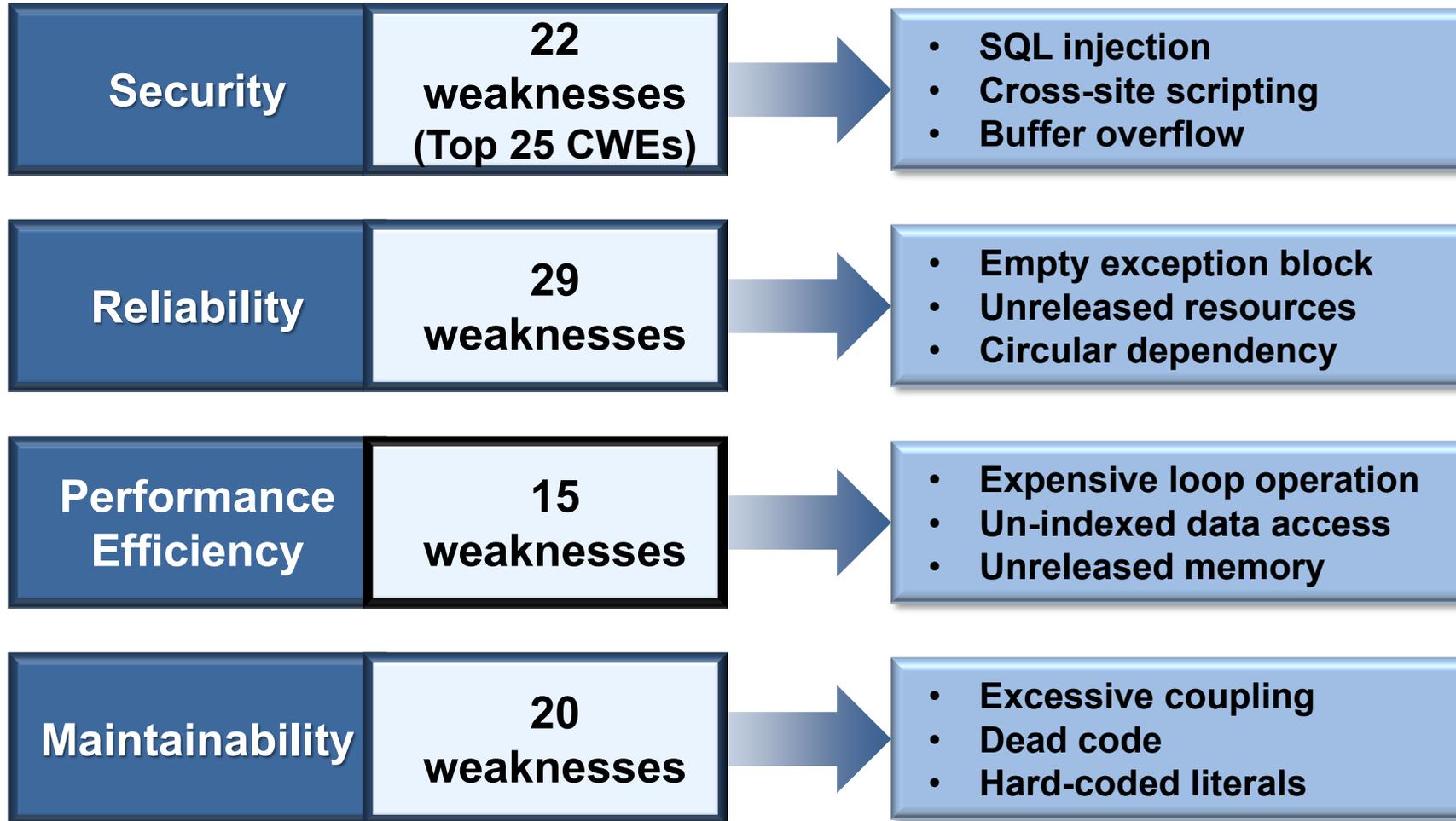


CISQ Partners





CISQ Structural Quality Measures



Example architectural and coding weaknesses included in the CISQ measures

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.

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.

CISQ measures conform to quality characteristic definitions in ISO/IEC 25010 and supplement measures in ISO/IEC 25023.



Recommendation

- ✓ Contact vendor delivery leaders to suggest they use CISQ measures for all ADM work



RFP

- ✓ Initial statement of requirements and project definition can list CISQ measures for assessing software quality



SLAs

- ✓ Treat software enhancements and maintenance as a service; track levels, penalties, credits



SOW

- ✓ Definition of specific project scope and deliverables can include specification of quality measures



Scorecard

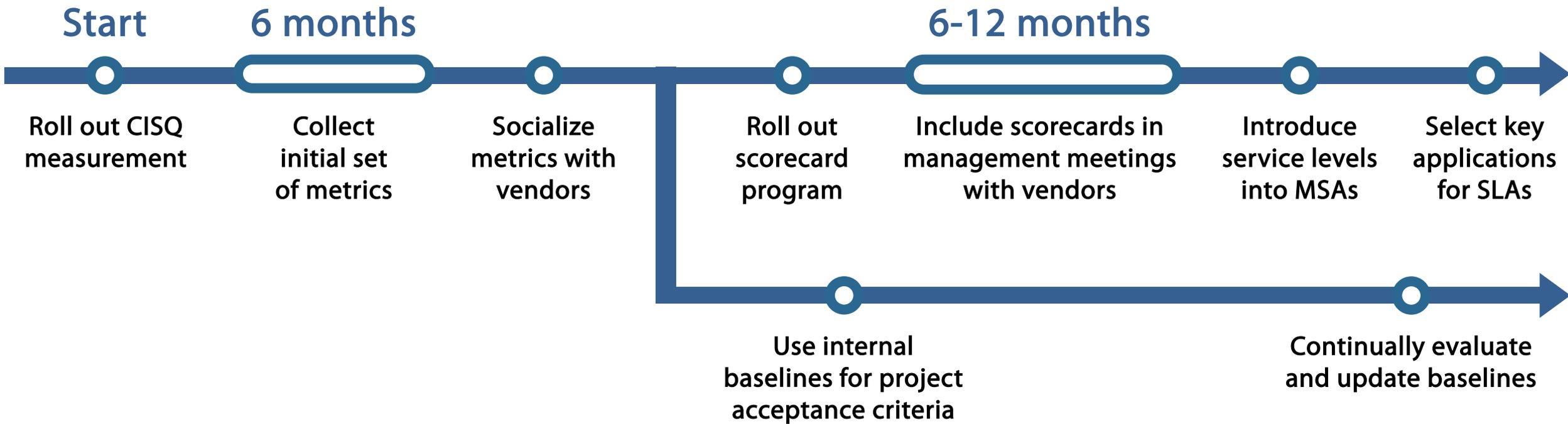
- ✓ Measurement and discussion in governance committees to ensure SLAs & KPIs are met

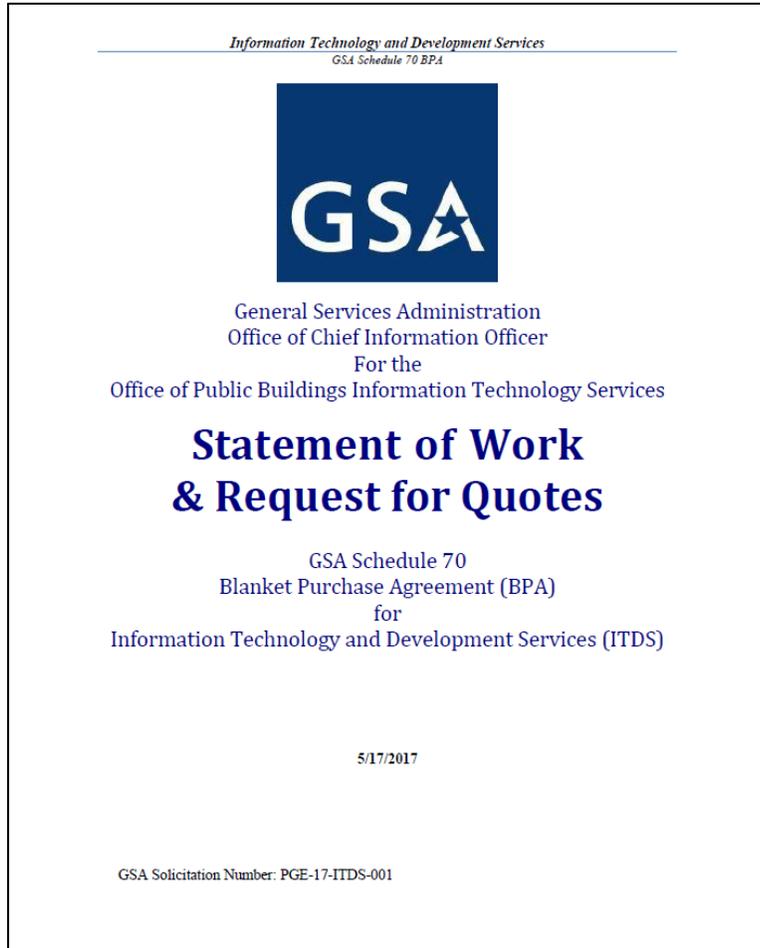


Acceptance criteria

- ✓ Demand minimal set of measurable acceptance criteria for any new development or release

Deploying a vendor measurement program is a process,
not a big bang event





CISQ has been referenced by the U.S. General Services Administration (GSA), formally citing CISQ requirements in a Information Technology (IT) statement of work from the Office of the CIO for the Office of Public Buildings. GSA is an independent agency of the U.S. government that supports general services of Federal agencies.

See page 21, section 5.9 in GSA’s document, Schedule 70 Blank Purchase Agreement for IT and Development Services...

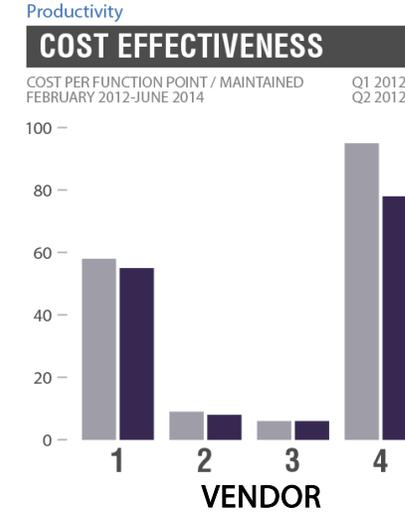
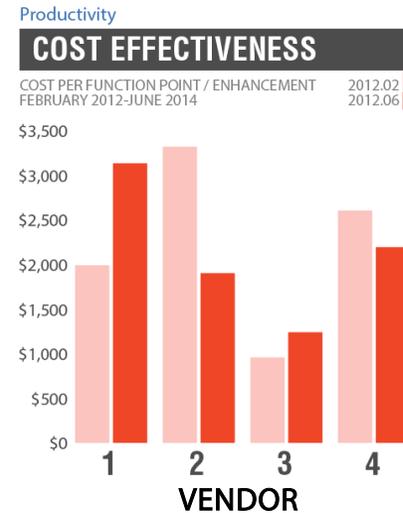
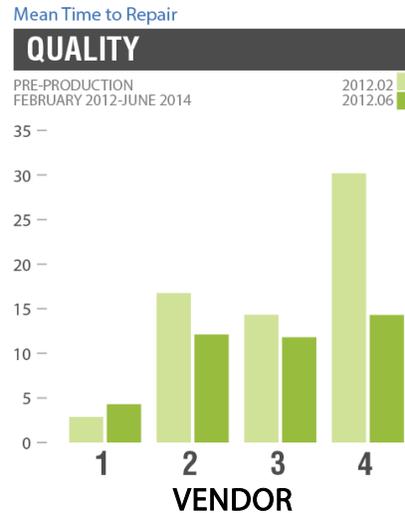
“PB-ITS (Project Based IT Services) is seeking to establish code quality standards for its existing code base, as well as new development tasks. As an emerging standard, PB-ITS references the Consortium for IT Software Quality (CISQ) for guidance on how to measure, evaluate and improve software.”

Scorecard Service Providers

	Reliability	Performance Efficiency	Security	Maintainability
VENDOR 1	3.16	2.34	3.01	1.99
VENDOR 2	2.78	3.38	3.12	2.34
VENDOR 3	1.67	3.54	2.98	1.76
VENDOR 4	3.12	3.11	2.79	3.11
VENDOR 5	3.56	3.88	3.03	3.42
VENDOR 6	3.76	2.89	2.97	2.55

Scores based on a 1 to 4 quality rating system

Monitor Performance Over Time



At Risk Amount and Allocation of Risk

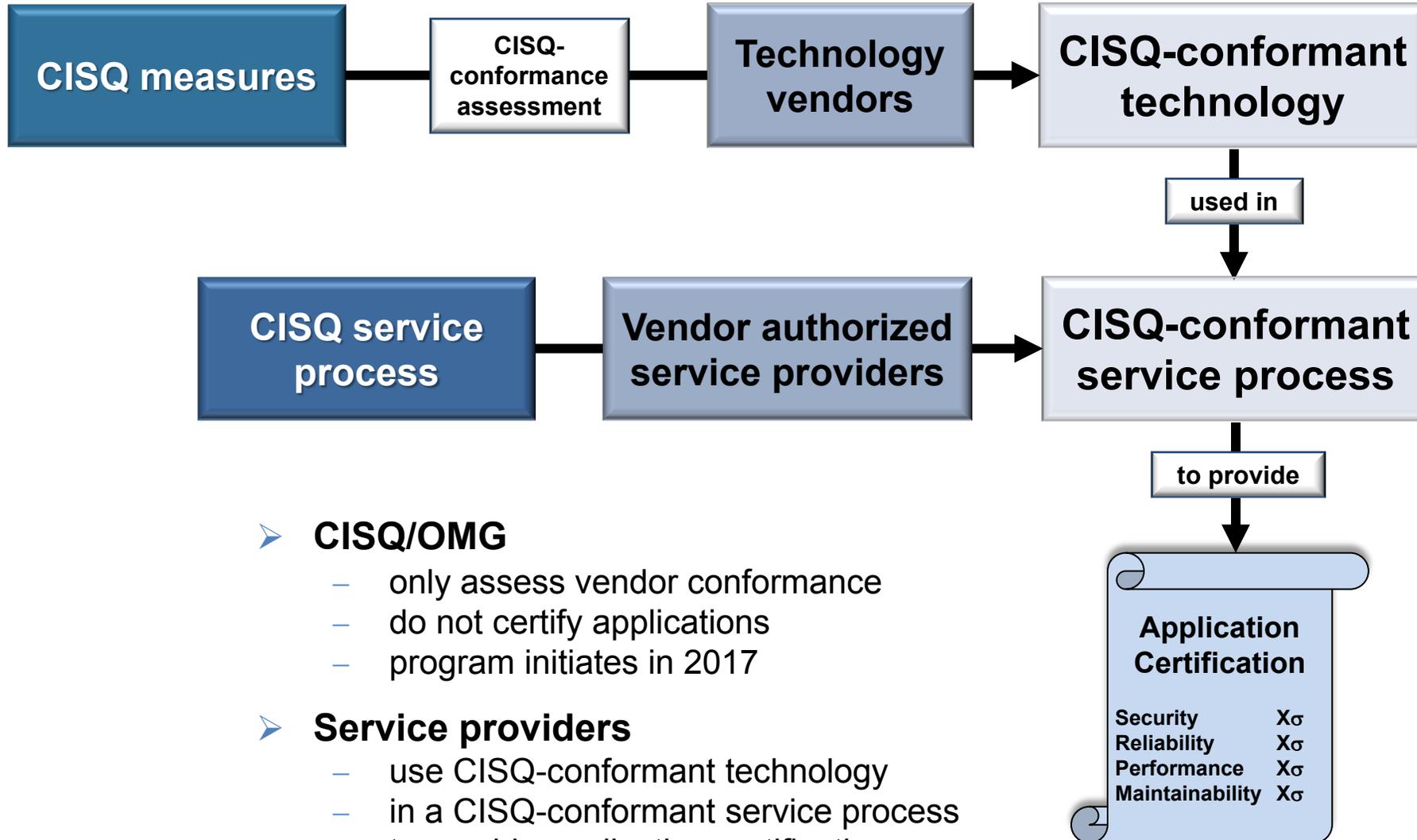
Total Billing Per Release : \$1,000,000
 Total At Risk Amount (10% of Bill) : \$100,000
 Total Risk Pooler: 100%

10% is for example

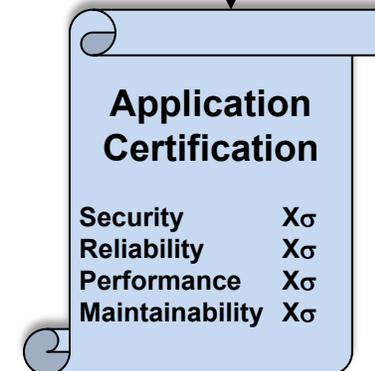
Application Name	Tier 1 Metrics (Critical Service Levels)	At Risk Multiplier	Risk Allocation	At Risk Amount
OMS	Security Findings	50%	30%	\$15,000
	Reliability Findings	30%		\$9,000
	Application Pain Violations	20%		\$6,000
		100%		\$30,000
CRM	Security Findings	30%	10%	\$3,000
	Reliability Findings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

Amount service provider has at risk on this individual Service Level is:
 $30\% * 50\% * \$100K = \$15,000$

- Any time there is a default, the at-risk amount will be forfeited
- Credits / Incentives are settled at the Annual Reset



- **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





Tracie Berardi

Program Manager

tracie.berardi@it-cisq.org

Website area for Vendor Management use case

- <http://it-cisq.org/vendor-management/>

Whitepaper about the concept of using CISQ metrics in SLAs

- <http://it-cisq.org/wp-content/uploads/2015/07/Using-Software-Measurement-in-SLAs-Integrating-CISQ-Size-and-Structural-Quality-Measures-into-Contractual-Relationships.pdf>

Whitepaper with detailed step-by-step instructions for putting CISQ metrics in SLAs

- <http://it-cisq.org/wp-content/uploads/2017/04/CISQ-Rec-Guide-Effective-Software-Quality-Metrics-for-ADM-Service-Level-Agreements.pdf>

Sample acceptance criteria using CISQ metrics

- <http://it-cisq.org/wp-content/uploads/2017/06/Sample-Acceptance-Criteria-with-CISQ-Standardized-Metrics.pdf>

Sample RFP from U.S. General Services Administration (GSA) that uses CISQ as part of it's requirement for quality software

- <http://it-cisq.org/wp-content/uploads/2017/06/ITDSBPASOWFINALV420170517.pdf>
- Go to section 5.9, page 21 of 73



Dr. Bill Curtis

Executive Director

bill.curtis@it-cisq.org

TRUSTWORTHY SYSTEMS MANIFESTO

We hold these truths to be self-evident

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 software-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

FOUNDED BY: Software Engineering Institute Carnegie Mellon, OBJECT MANAGEMENT GROUP®

Standards Programs Use Cases Members Area Events About CISQ Embedded WG

FAQs Contact Us

Search

Member Login

Facebook Twitter LinkedIn YouTube

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.

Attend the CISQ & IAOP webinar on February 6, [How Can VMOs Ensure Vendor-Supplied Software is Trustworthy?](#), presented by Dr. Bill Curtis, CISQ Exec Director.

Become a CISQ:

Member → CISQ Members Area

Sponsor → CISQ Events

CISQ Sponsors



Trustworthy Systems Manifesto

5 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

WE HOLD THESE TRUTHS TO BE SELF-EVIDENT

SIGN IT TODAY!

CISQ Consortium for IT Software Quality™

#TrustworthyManifesto

Over 2000 individual members from large software-intensive organizations:



