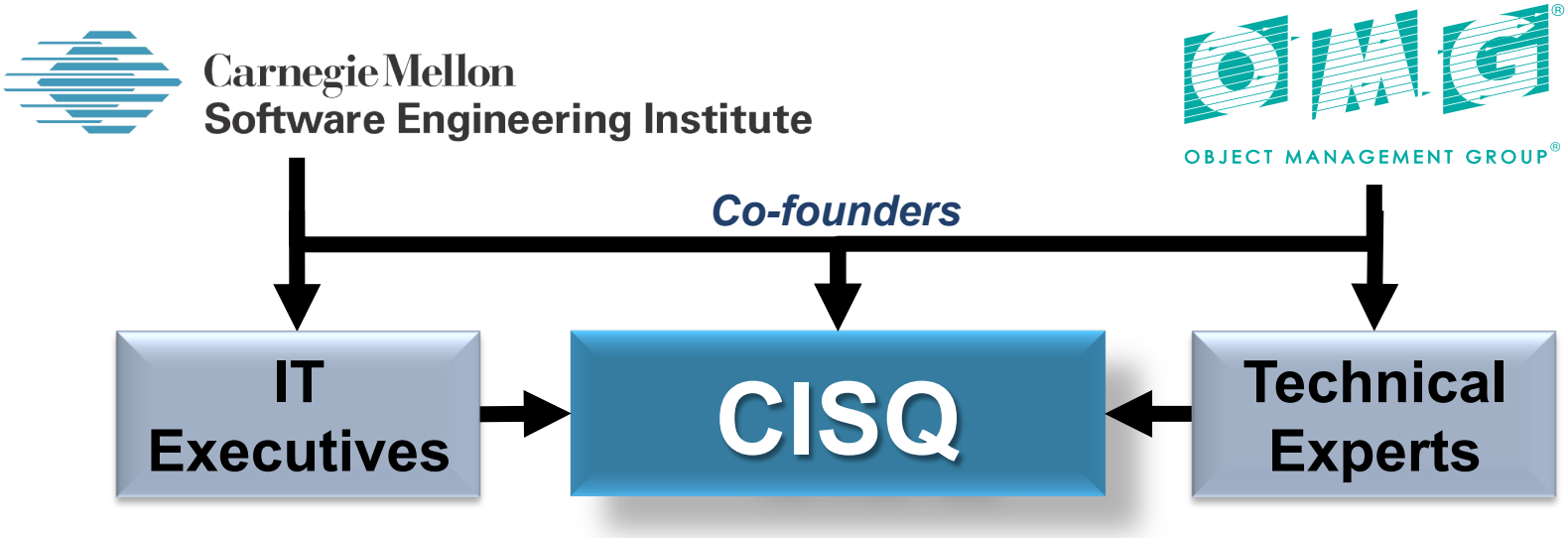
CISQ Measures of Secure, Resilient Software

OMG Standards for Software Measurement

Dr. Bill Curtis
Executive Director, CISQ

CISQ
Consortium for IT Software Quality

What is CISQ?



OMG Special Interest Group

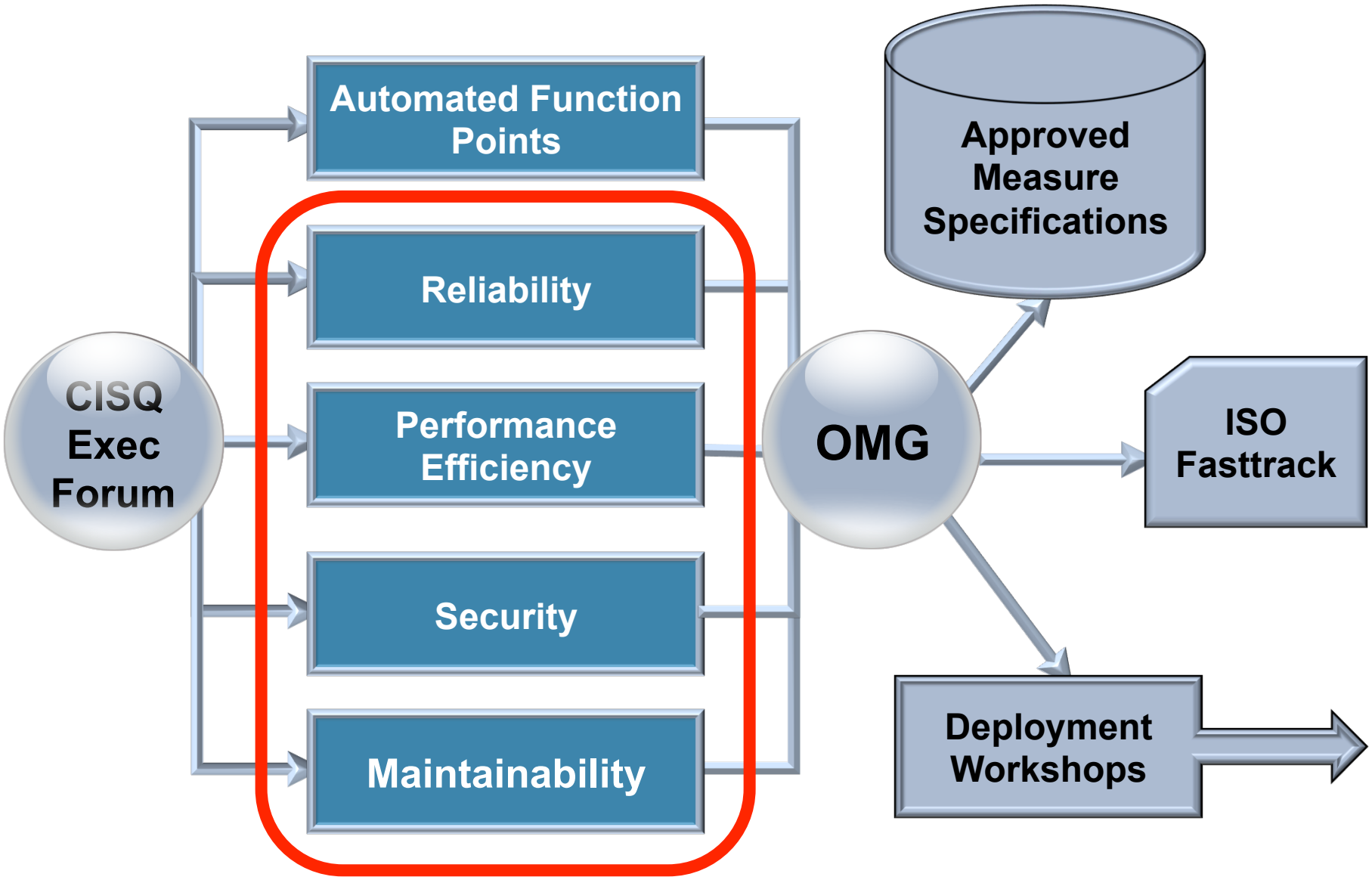
CISQ is chartered to define automatable measures of software size and quality that can be measured in the source code, and promote them to become Approved Specifications of the OMG®

CISQ Sponsors

accenture
Cognizant
Booz | Allen | Hamilton
strategy and technology consultants
SYNOPSYS®
CAST
ACHIEVE INSIGHT. DELIVER EXCELLENCE.
HUAWEI

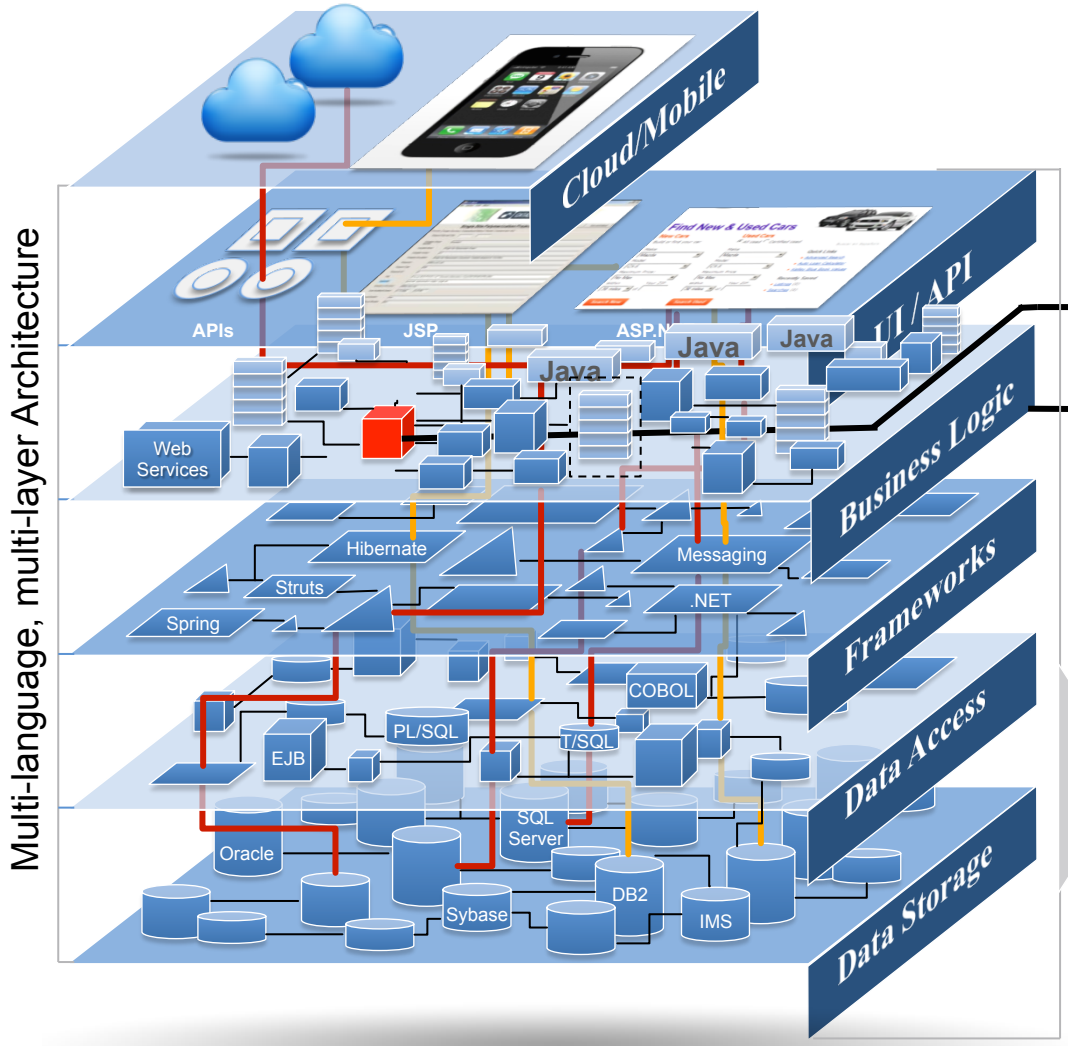
CISQ
Consortium for IT Software Quality

CISQ Measurement Standards



CISQ
Consortium for IT Software Quality

Measuring the Technology Stack



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

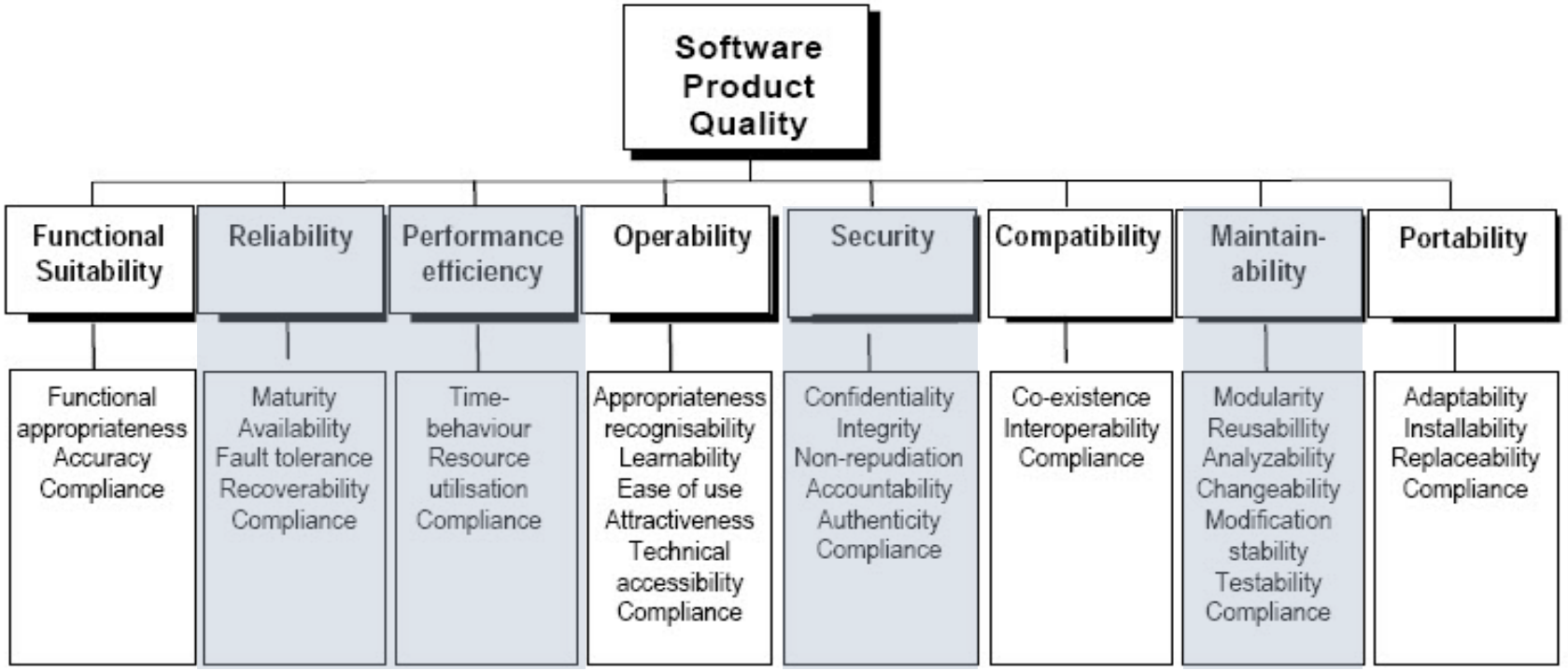
3 System Level

- 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
Consortium for IT Software Quality

Relating CISQ Measures 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



CISQ defined automatable measures for quality characteristics highlighted in blue

CISQ
Consortium for IT Software Quality

CISQ Measures Violations

CISQ Quality Characteristic Measures		Example violations of good architectural and coding practice that compose the CISQ measures
Security	22 violations (Top 25 CWEs)	• SQL injection • Cross-site scripting • Buffer overflow
Reliability	29 violations	• Empty exception block • Unreleased resource • 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

CISQ Consortium for IT Software Quality — Security Measure — Top 22 CWEs

- 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

Common Weakness Enumeration

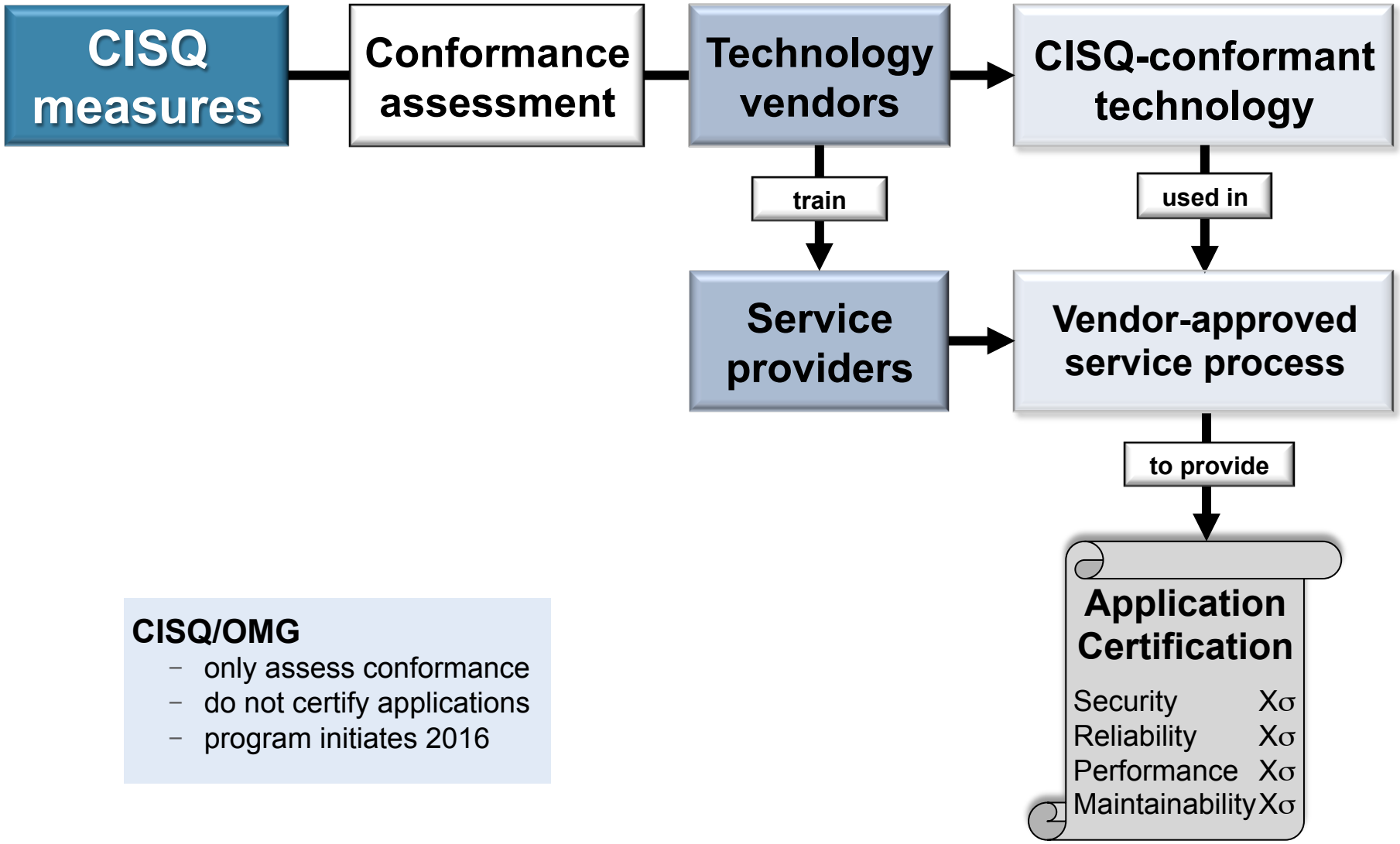
cwe.mitre.org

CISQ
Consortium for IT Software Quality

Issue → Quality Rule → Measure Element

Issue	Quality Rule	Quality Measure Element
CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	**Rule 1:** Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid, such as Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket.	**Measure 1:** # of instances where output is not using library for neutralization
CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	**Rule 2:** Use a vetted library or framework that does not allow SQL injection to occur or provides constructs that make this SQL injection easier to avoid or use persistence layers such as Hibernate or Enterprise Java Beans.	**Measure 2:** # of instances where data is included in SQL statements that is not passed through the neutralization routines.

CISQ Conformance and App Certification



CISQ/OMG

- only assess conformance
- do not certify applications
- program initiates 2016

www.it-cisq.org

Consortium for IT Software Quality

- **Membership is free**
- **Measurement standards**
- **White papers, blogs**
- **Structural quality resources**

Automated FPs	http://www.omg.org/spec/AFP/
Security	http://www.omg.org/spec/ASCSM/
Reliability	http://www.omg.org/spec/ASCRM/
Performance	http://www.omg.org/spec/ASCPEM/
Maintainability	http://www.omg.org/spec/ASCMM/