

# Technical Debt: An Automatable Standard

Marc Jones,  
Federal Director CISQ (vol.)  
13Dec17 – SSCA  
[marc.jones@it-cisq.org](mailto:marc.jones@it-cisq.org)



## H.R. 3304

Directs the Secretary to provide for the establishment of a joint federation of capabilities to support the trusted defense system needs (security of software and hardware) of DOD. Requires the Secretary to determine whether the federation's purpose can be met by existing centers within DOD and, if not, to devise a strategy for creating and providing resources to fill such gaps.

### SEC. 937. JOINT FEDERATED CENTERS FOR TRUSTED DEFENSE SYSTEMS FOR

#### THE DEPARTMENT OF DEFENSE.

**...the requirements for**

**the discharge by the**  
**federation, in**  
**coordination with the**

**Center for Assured**  
**Software of the National**  
**Security Agency, of a**

**program of research and**  
**development to improve**  
**automated software code**  
**vulnerability analysis and**  
**testing tools**

## H.R. 4310

Directs the Under Secretary to: (1) develop and implement a baseline software assurance policy for the entire lifecycle of computer software acquired for DOD critical information, business, and weapons systems; (2) collect data on, and measure the effectiveness of, such policy; and (3) brief the defense and appropriations committees on additional means of improving software assurance and vulnerability detection.

### SEC. 933. IMPROVEMENTS IN ASSURANCE OF COMPUTER SOFTWARE PROCURED

#### BY THE DEPARTMENT OF DEFENSE.

**....shall develop and implement a**  
**baseline software assurance**  
**policy for the entire lifecycle of**  
**covered systems....**

**(4) ...promote**

**best practices and standards to**

**achieve software**

**security, assurance,**

**and quality ...**

(1) require use of appropriate automated vulnerability analysis tools in computer software code during the entire lifecycle of a covered system, including during development, operational testing,



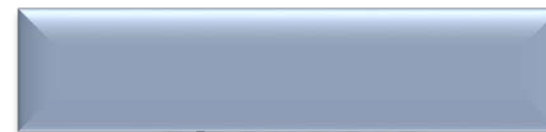
**Carnegie Mellon  
Software Engineering Institute**



*Co-founders*



<b>OMG Special Interest Group</b>	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®
---	---



Booz | Allen | Hamilton



Cognizant

**SYNOPSYS®**



ACHIEVE INSIGHT. DELIVER EXCELLENCE.



## 5.9 Quality Requirements (Task Area 15)

The Enterprise Quality Program (EQP), provides the foundation for continuously improving, managing, and controlling the quality of software products for PB-ITS. Contractors shall follow PB-ITS Enterprise Quality Program (EQP) standards and practices. All deliverables shall be produced and delivered in accordance with PB-ITS's current EQP requirements provided in the Enterprise Quality Configuration Management Plan and the Release Matrix in Appendix A. The Government PM shall notify the Contractors, verbally or in writing, of deficiencies in the quality of deliverables and allow five (5) business days for a revision to be submitted.

PB-ITS 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) (<http://it-cisq.org/standards/>) for guidance on how to measure, evaluate and improve software. Particular areas of importance are Performance Efficiency, Reliability, Maintainability and Security. Contractors shall perform architectural and coding best practices within their development environments in order to deliver efficient, secure and reliable products to the Government. GSA currently uses a suite of tools and processes to assess the efficiency, security and reliability of code in applications.**



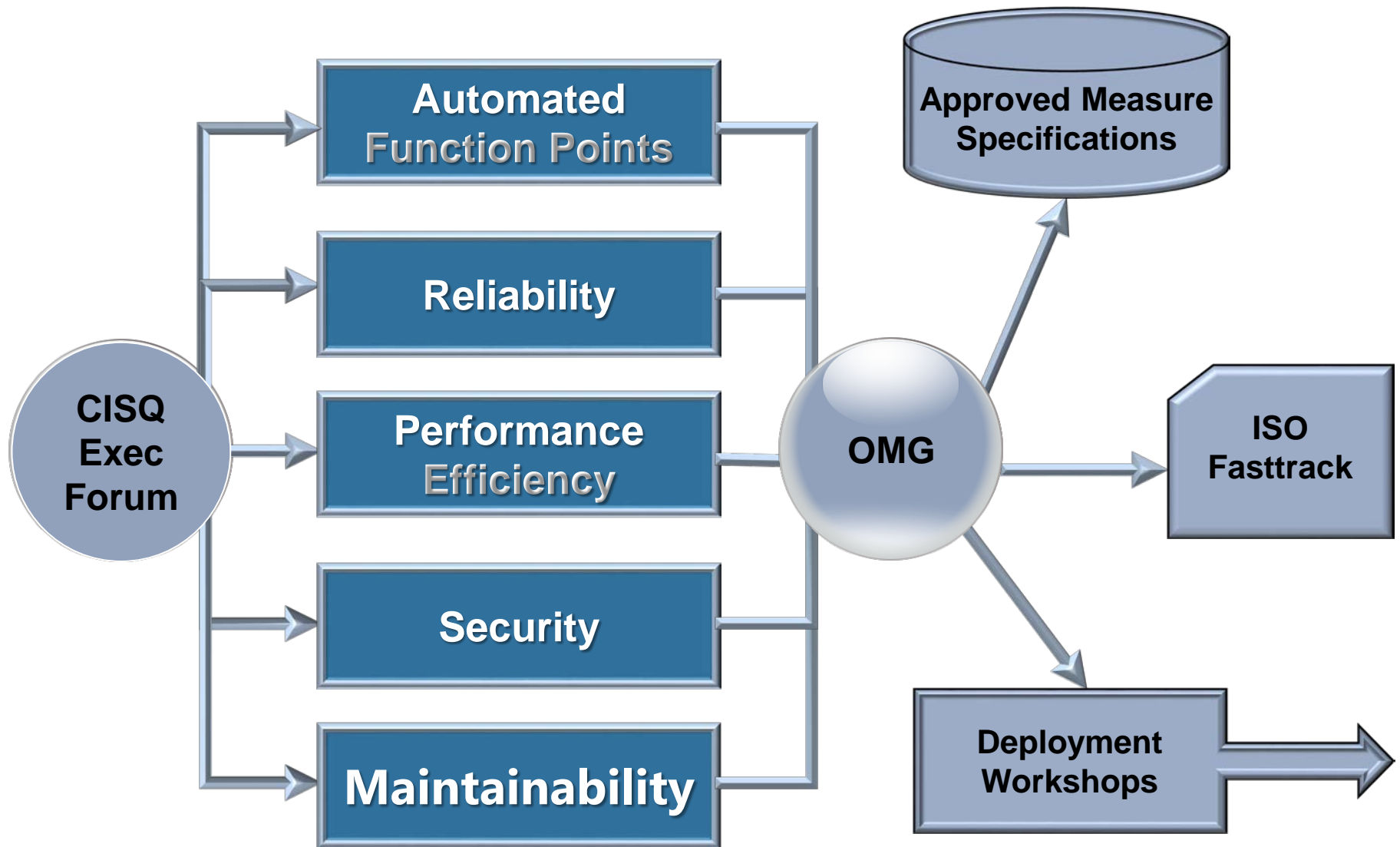
The Contractor shall adhere to CST application coding standards intended to assist in creating code that is free of critical quality defects and is highly maintainable.

CST will employ a Software Code Review process by which it will analyze all source code by measuring application level code quality and code assurance across the portfolio of COTS configurations and custom developed software. **CST will also employ Software Code Quality (SCQ), an analysis that will evaluate application risk around robustness (stability, resiliency), performance, architectural security, transferability, system maintainability (sustainment) and changeability of applications as they evolve. These measurements are based upon industry best practices and standards related to complexity, programming practices, architecture, database access and documentation. They are derived from standards bodies such as the International Organization for Standardization (ISO), Software Engineering Institute (SEI), Object Management Group (OMG) and the National Institute of Standards and Technology among others.**

CST will leverage static code analysis tools, including **CAST Software's Application Analytics and Engineering Dashboards** with quality as its main focus to expose quality defects and ensure that code complies with established code quality metrics across all source language components that comprise the complete deployable software modules delivered under this base IDIQ and associated task orders issued thereunder.

Business capability.

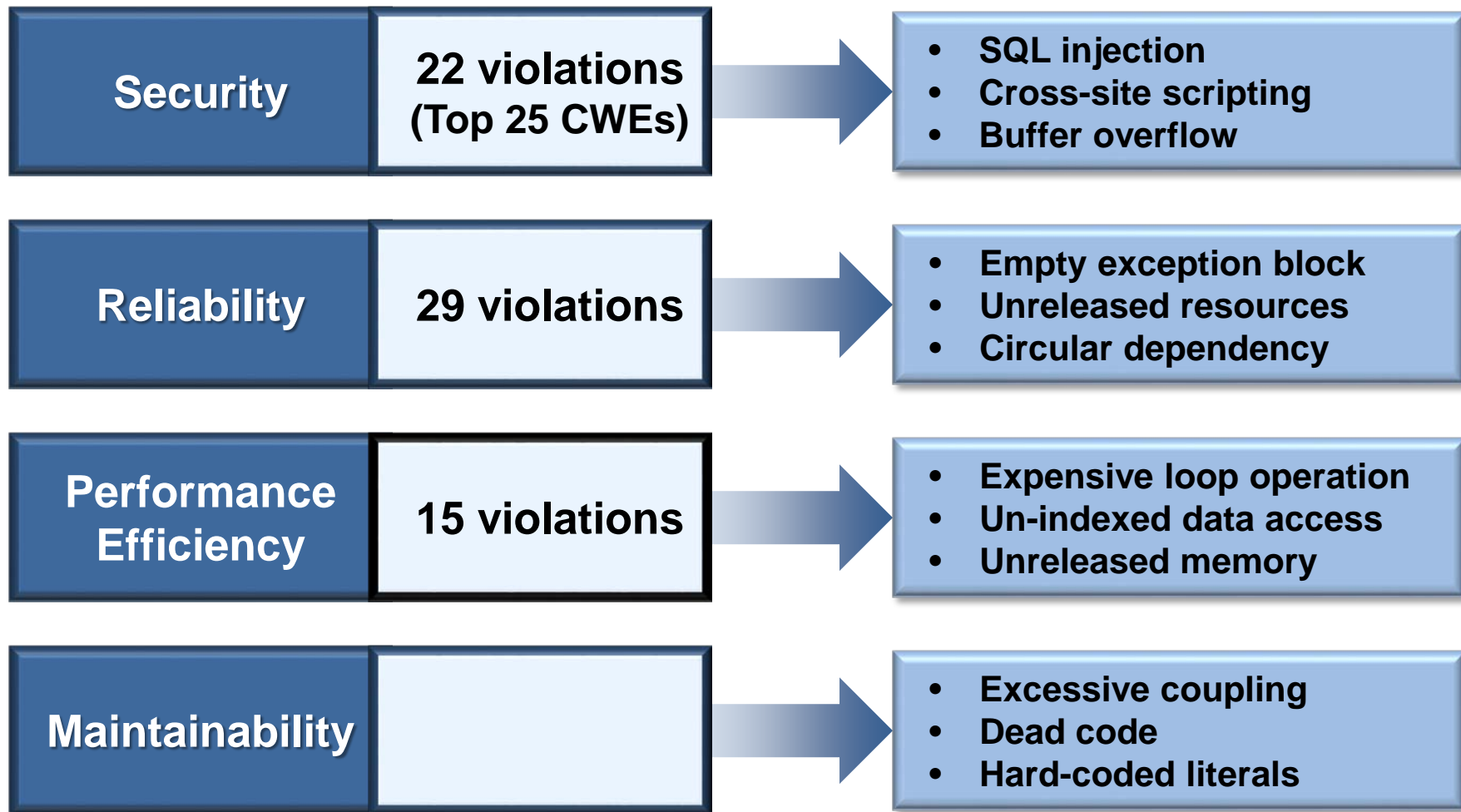






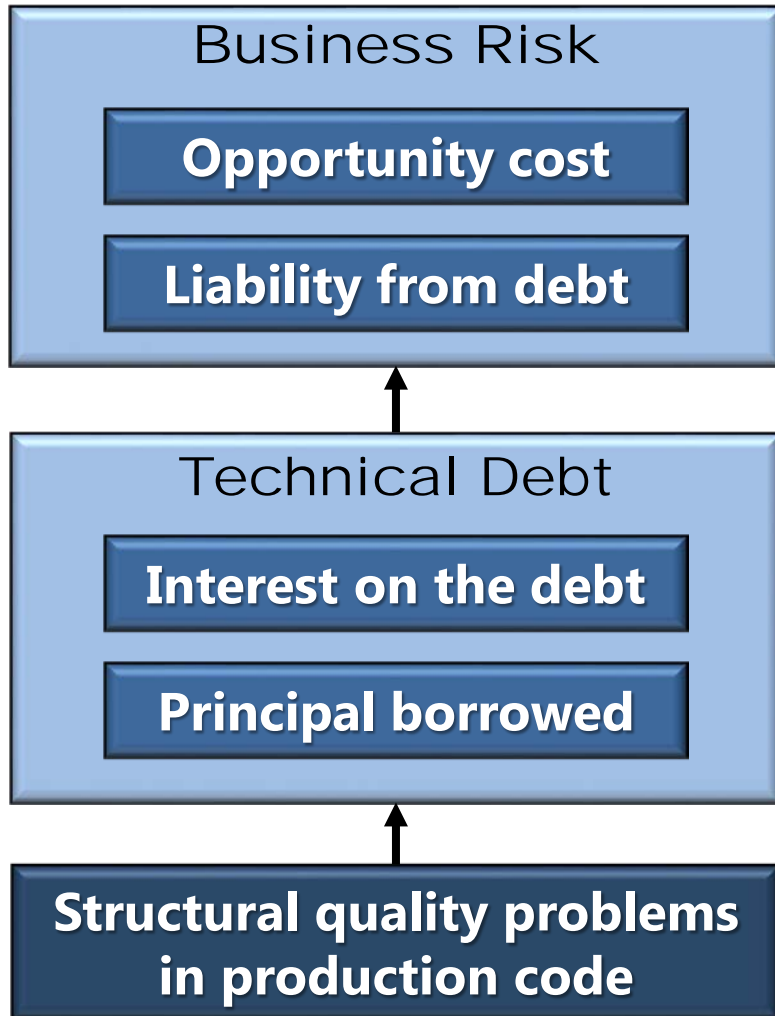
## CISQ Quality Characteristic Measures

## Example architectural and coding violations composing the CISQ measures



## The Technical Debt Metaphor

Technical Debt — **the future cost of defects remaining in code at release, a component of the cost of ownership**



**Opportunity cost**—benefits that could have been achieved had resources been put on new capability rather than retiring technical debt

**Liability**—business costs related to outages, breaches, corrupted data, etc.

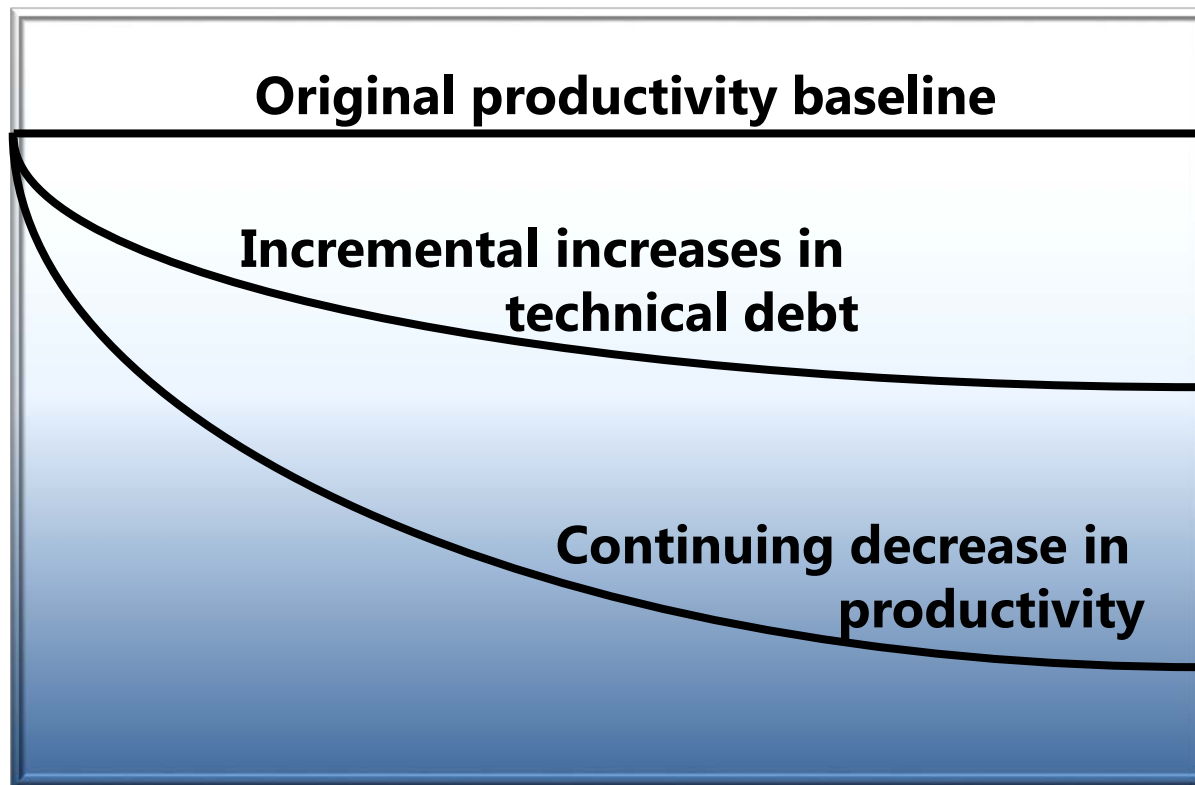
**Interest**—continuing IT costs attributable to the violations causing technical debt, i.e, higher maintenance costs, greater resource usage, etc.

**Principal**—cost of fixing problems remaining in the code after release that must be remediated

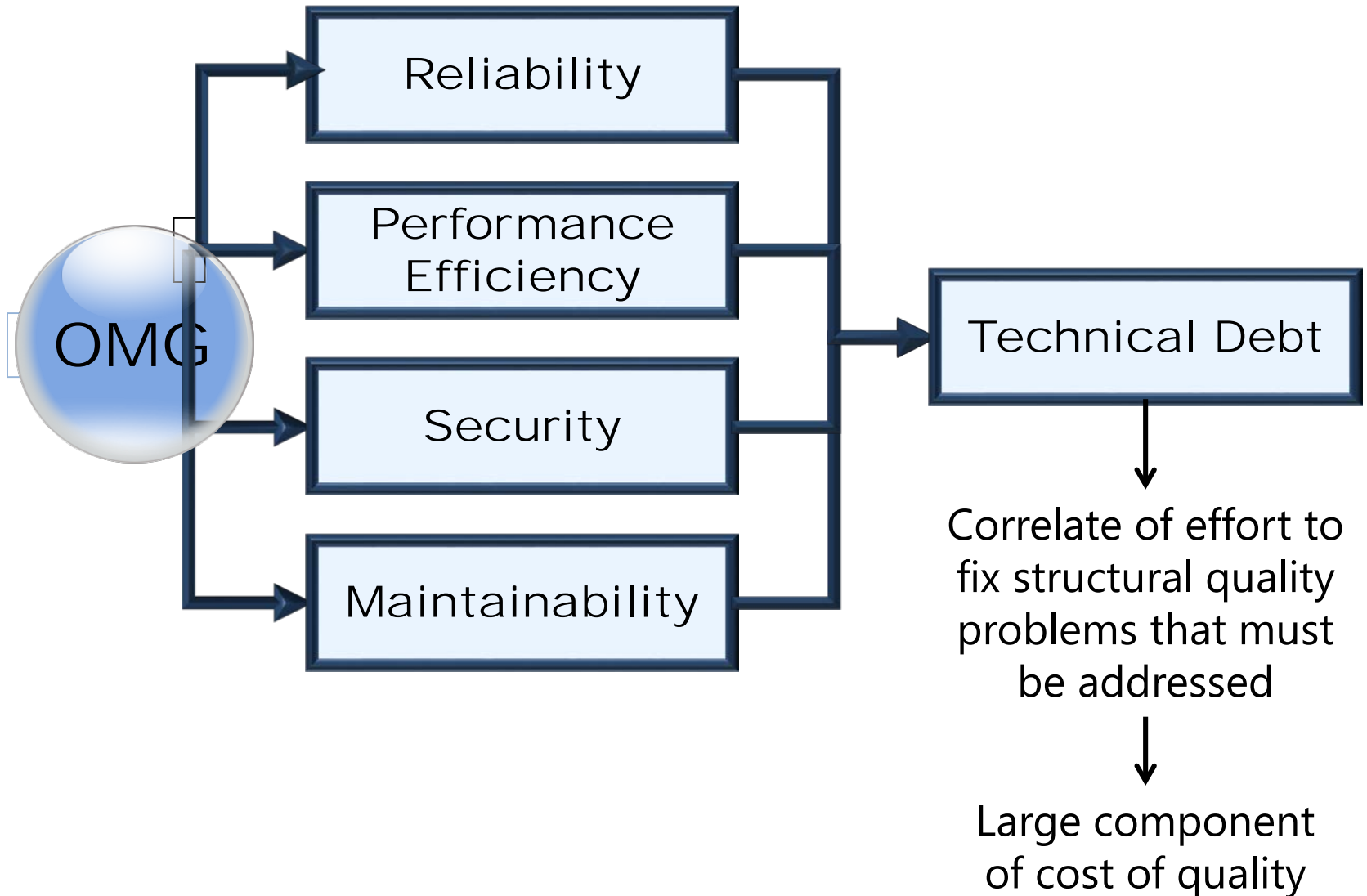
# How Quality Affects Productivity

Assumption: Productivity is a stable number

Reality: Productivity is a monotonically decreasing function of releases



Unless you take action !!!





# Automated Technical Debt Measure

**AUTOMATED TECHNICAL DEBT MEASURE**

$\Sigma$  all four quality characteristics

**QUAL. CHARAC. REMEDIATION EFFORT MEASURE**

$\Sigma$  all weaknesses in a quality characteristic

**WEAKNESS REMEDIATION EFFORT**

$\Sigma$  all occurrences of a weakness

**OCCURRENCE REMEDIATION EFFORT**

$\Sigma$  for each occurrence of a weakness

**OCCURRENCE RAW REMEDIATION EFFORT**

(based on survey results)

**ADJUSTMENT FACTOR**

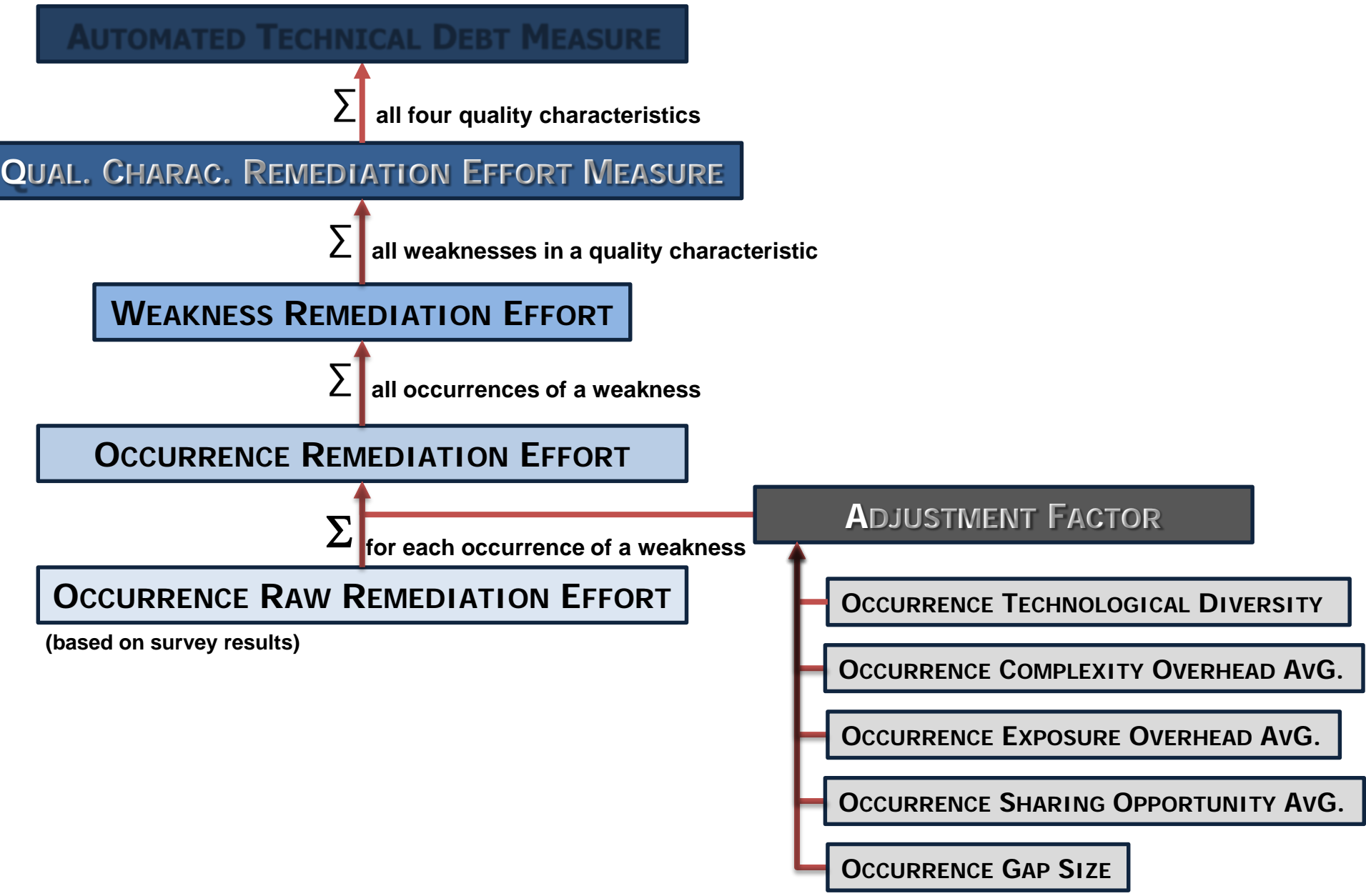
OCCURRENCE TECHNOLOGICAL DIVERSITY

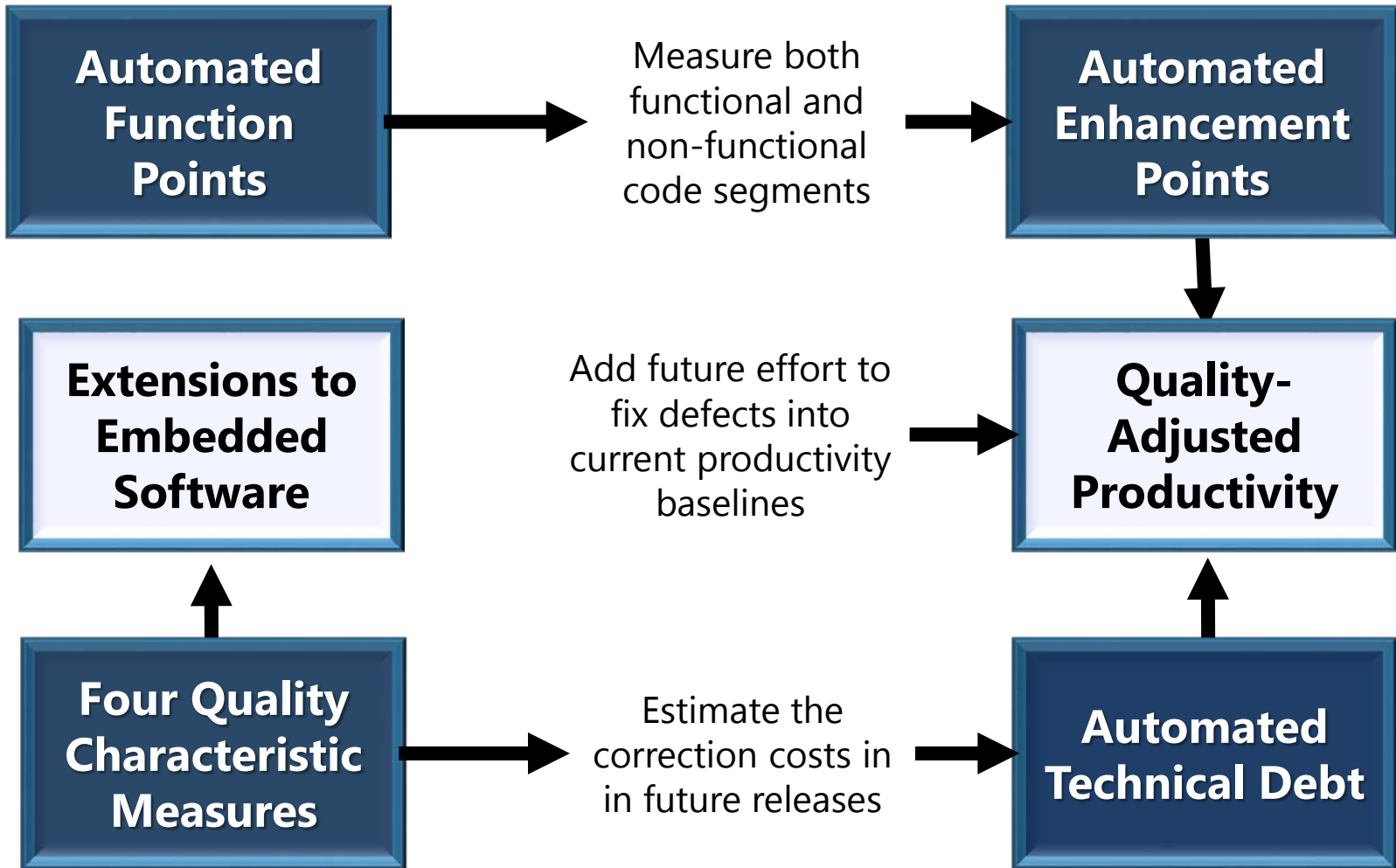
OCCURRENCE COMPLEXITY OVERHEAD AVG.

OCCURRENCE EXPOSURE OVERHEAD AVG.

OCCURRENCE SHARING OPPORTUNITY AVG.

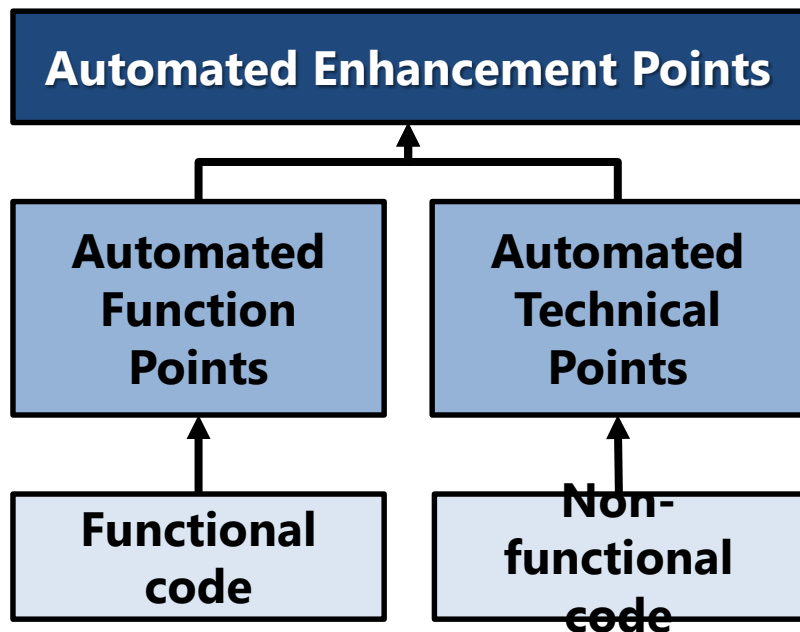
OCCURRENCE GAP SIZE








- IT shops found that automated or manual Function Points had severe limitations in productivity analysis → did not include the size of non-functional code
- The Automated Enhancement Points specification measures both and integrates them into one size measure



An OMG® Automated Enhancement Points Publication



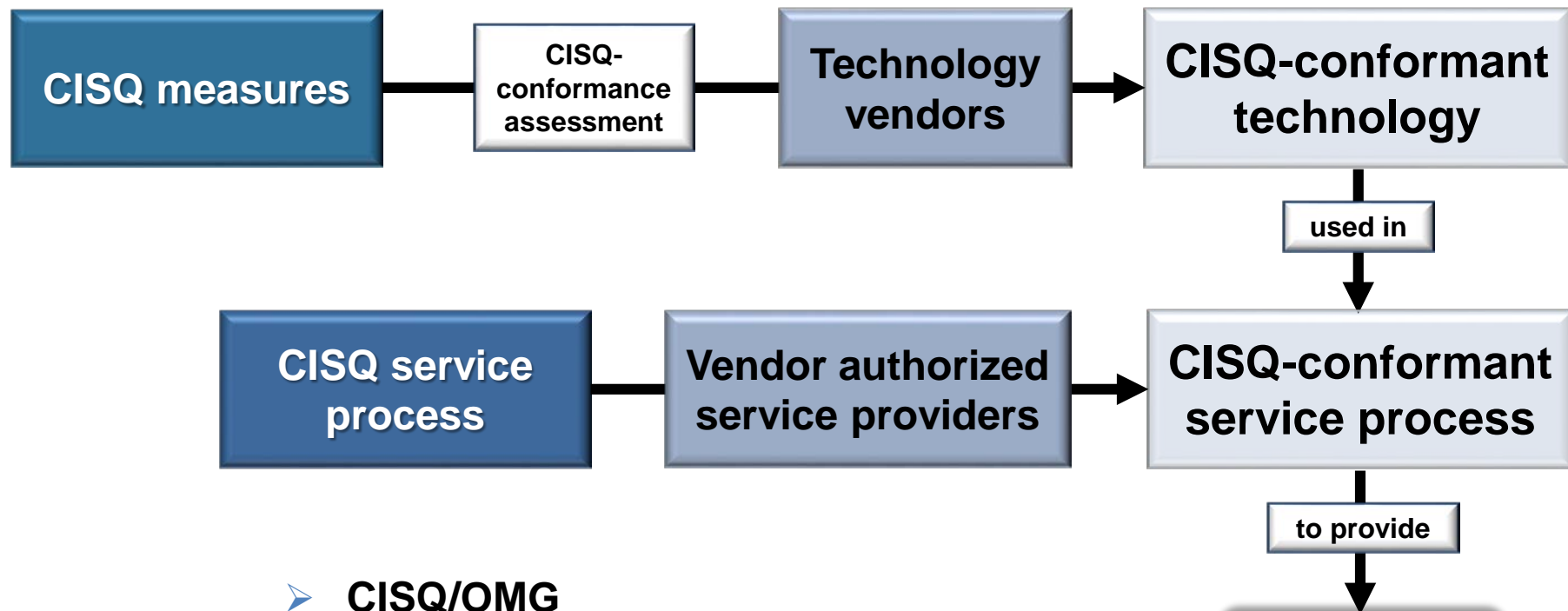
## Automated Enhancement Points

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.xml>

---



## ➤ 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

### Application Certification

Security	X $\sigma$
Reliability	X $\sigma$
Performance	X $\sigma$
Maintainability	X $\sigma$

## October 2017 Semi-Annual Meeting



Announcing Webinar:  
**CISQ Webinar:**  
**New Automated Technical Debt Standard**  
**Dr. Bill Curtis, Executive Director, CISQ**  
**January 16, 2018**  
**11:00am – 11:30am ET**

8:30	<p><b>Welcome Remarks</b></p> <ul style="list-style-type: none"> <li>– Dr. Bill Curtis, Executive Director, Consortium for IT Software Quality (CISQ)</li> <li>– John Weiler, Vice Chair, IT Acquisition Advisory Council (IT-AAC)</li> </ul>
8:45	<p><b>Opening Keynote Panel</b></p> <ul style="list-style-type: none"> <li>– Tony Scott, former Federal Chief Information Officer</li> <li>– Greg Smithberger, CIO/CTO, NSA</li> </ul>
9:15	<p><b>Titans of Cyber Panel: Policy and Directives for Modernizing and Securing Legacy IT</b>  <b>Topics: FITARA, MGT Act, Executive Order for Cyber Security</b>  <b>Lead: Dr. Edward E. Amoroso, CEO, Tag Cyber LLC</b></p> <ul style="list-style-type: none"> <li>– Jeffrey Eisensmith, CISQ, DHS OCIO</li> <li>– Sara Mosley, Acting Director for the Office of the Chief Technology Officer, DHS CS&amp;C</li> <li>– Jack Wilmer, Cyber lead for American Technology Council, White House OSTP</li> <li>– Ken Bible, Deputy CIO, U.S. Marine Corps</li> </ul>
10:30	<p><b>Break &amp; Networking</b></p>
10:45	<p><b>Standards to Measure and Manage Security, Resilience and Technical Debt</b></p> <ul style="list-style-type: none"> <li>– Dr. Bill Curtis, Executive Director, Consortium for IT Software Quality (CISQ)</li> <li>– John Weiler, Vice Chair, IT Acquisition Advisory Council (IT-AAC)</li> </ul>
11:25	<p><b>Cyber Resilience Standards of Practice</b>  <b>Lead: Dr. Bill Curtis, Executive Director, Consortium for IT Software Quality (CISQ)</b></p> <ul style="list-style-type: none"> <li>– Dr. Ron Ross, Computer Scientist and Fellow, NIST</li> <li>– Roberta Stempfley, Director of SEI's CERT Division</li> <li>– Herb Krasner, University of Texas at Austin (ret.), Texas IT Champion</li> </ul>
12:15	<p><b>Luncheon and Networking</b></p>
12:45	<p><b>Luncheon Keynote: Defense Cyber Way Forward</b></p> <ul style="list-style-type: none"> <li>– Dr. Thresa Lang, Deputy Director, Navy Cybersecurity/Deputy Director, Department of the Navy Deputy Chief Information Officer (Navy)</li> </ul>
1:15	<p><b>Titans of Cyber Panel: Best Practices and Innovations for Rapid, Secure Modernization</b>  <b>Lead: John Weiler, Vice Chair, IT Acquisition Advisory Council (IT-AAC)</b></p> <ul style="list-style-type: none"> <li>– Therese Firmin, Principal Director, DCIO (CS) and Deputy Chief Information Security Officer, Department of Defense</li> <li>– Jose Arrieta, Director, Office of IT 70 Schedule Contract Operations, GSA</li> <li>– Brigadier General (ret) Greg Touhill, former U.S. CISQ; President of Cyxtera Federal Group</li> <li>– Matt Conner, CISQ, National Geospatial-Intelligence Agency</li> </ul>
2:15	<p><b>Supply Chain and Integration Risk Management</b>  <b>Lead: Joe Jarzombek, Global Manager, Synopsys Software Integrity Group</b></p> <ul style="list-style-type: none"> <li>– Emile Monette, Senior Cybersecurity Strategist and Acquisition Advisor, DHS Continuous Diagnostics and Mitigation Program</li> <li>– Shon Lyublanovits, IT Security Category Manager and Director of the Security Services Division for the Office of Integrated Technology Services (ITS) in GSA's Federal Acquisition Service (FAS)</li> <li>– Dave Duma, Acting Director, Operational Test and Evaluation, Department of Defense</li> </ul>





Consortium for IT Software Quality

FOUNDED BY:




[FAQs](#) [Contact Us](#)

[Member Login](#)




Standards
Programs
Use Cases
Members Area
Events
About CISQ

## Consortium for IT Software Quality

The Consortium for IT Software Quality™ (CISQ™) is an IT industry leadership group comprised of IT executives from the Global 2000, system integrators, outsourced service providers, and software technology vendors committed to introducing computable metrics standards for measuring software quality & size. CISQ is a neutral, open forum in which customers and suppliers of IT application software can develop an industry-wide agenda of actions for improving IT application quality to reduce cost and risk.

Link to [Knowledge Repository](#) from the Oct 19 Cyber Resilience Summit in Arlington, VA



Become a CISQ:

Member

→

CISQ Members Area

Sponsor

→

CISQ Events

### CISQ Sponsors



**SAVE THE DATE: ANNOUNCING THE DATE FOR THE SPRING EVENT**

## Cyber Resilience Summit

March 20, 2018 in Reston, VA U.S.A.

CO-PRODUCED BY:

