CISQ

Consortium for IT Software Quality™

Update on CISQ and ISO 25010

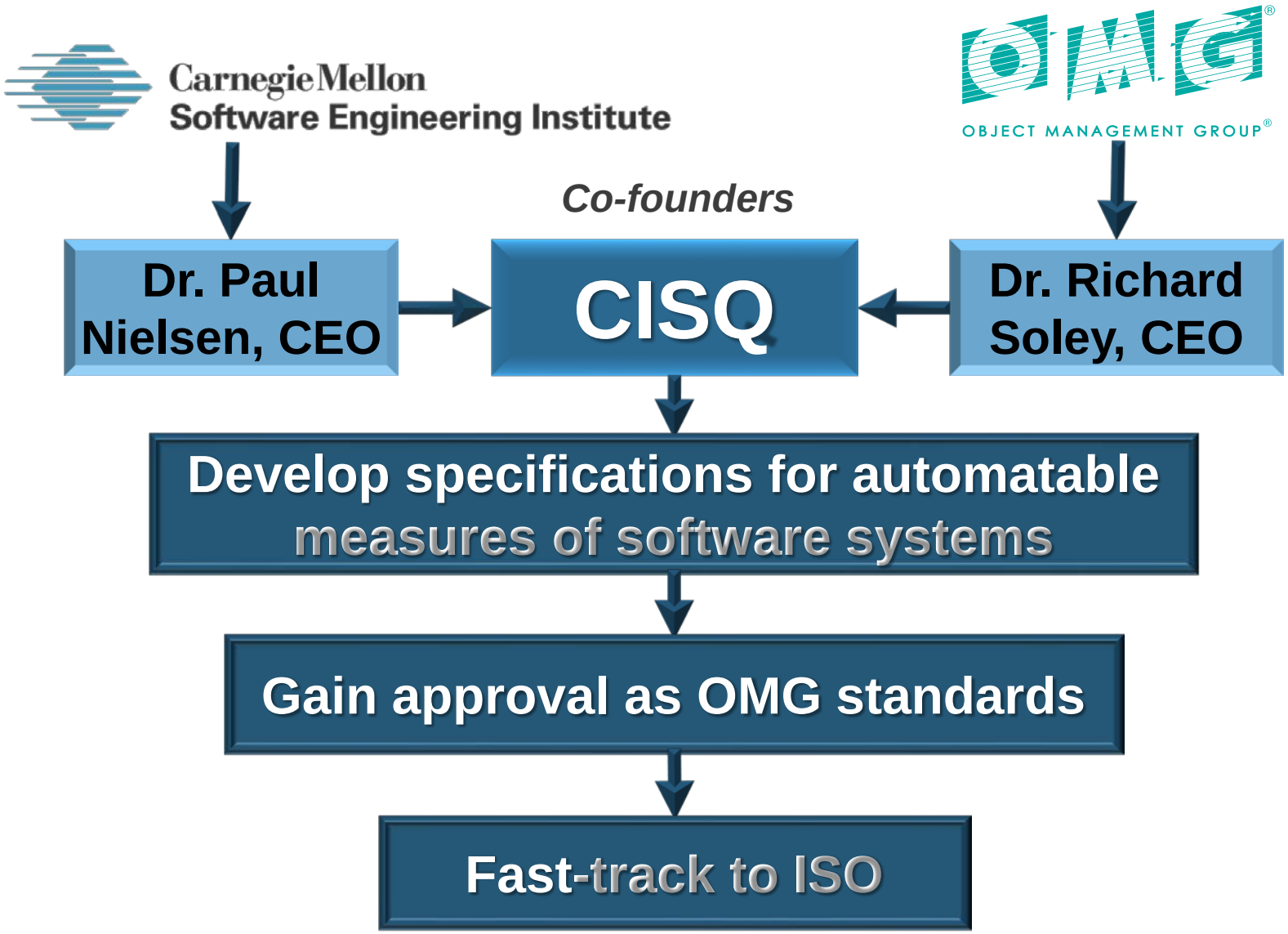
Dr. Bill Curtis

Founding Executive Director, CISQ

SSCA, McClean, VA

May 8, 2019

What Is the Consortium for IT Software Quality ?



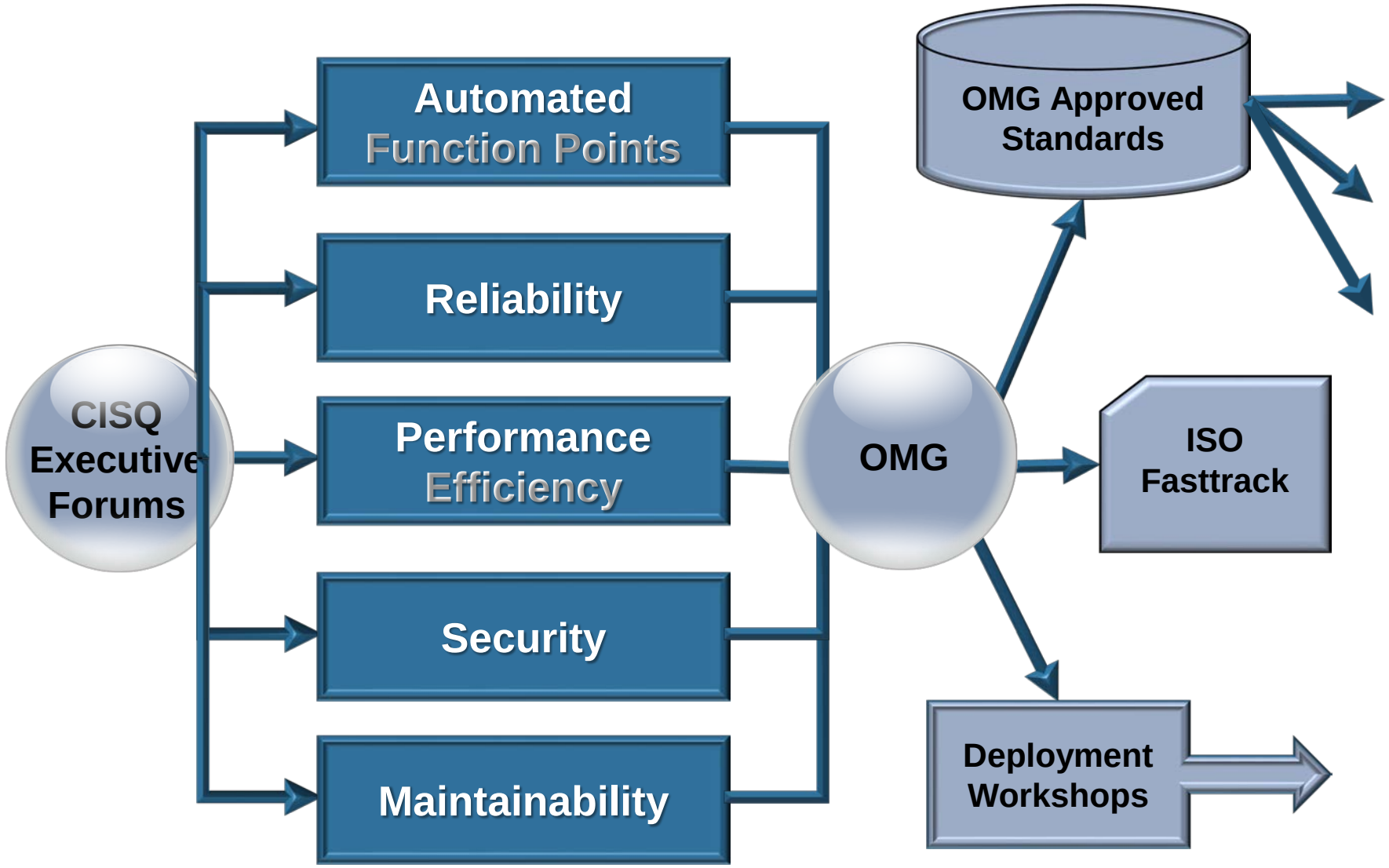
CISQ Sponsors

Cognizant
SYNOPSYS®
Tech Mahindra
SHPI
CAST
CGI
NORTHROP GRUMMAN

CISQ Partners

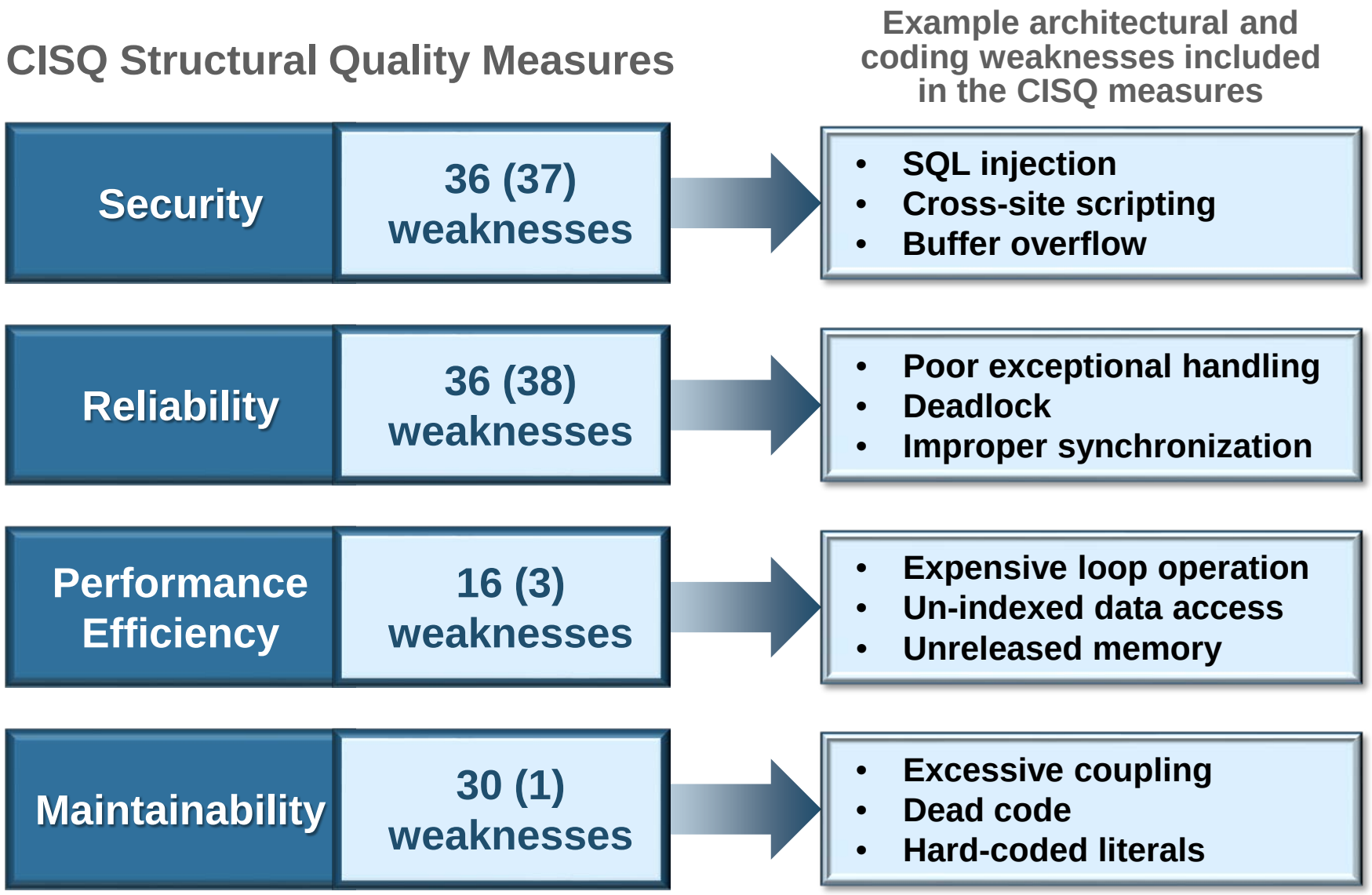
Gartner
QuEST FORUM
FORRESTER®
IAOP
ITAAC
TECHWELL
AFCEA WASHINGTON, DC CHAPTER
MAKING SOFTWARE BETTER

CISQ/OMG Standards Process



CISQ Structural Quality Measures

Consortium for IT Software Quality



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 they must be remediated were included in the CISQ measures.

CISQ Structural Quality measures have been extended to embedded systems software

CISQ Measures Updated for Embedded Systems

Consortium for IT Software Quality

CWE #	Descriptor	Weakness description
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	The software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory.
CWE-23	Relative Path Traversal	The software uses external input to construct a pathname that should be within a restricted directory, but it does not properly neutralize sequences such as ".." that can resolve to a location that is outside of that directory.
CWE-36	Absolute Path Traversal	The software uses external input to construct a pathname that should be within a restricted directory, but it does not properly neutralize absolute path sequences such as "/abs/path" that can resolve to a location that is outside of that directory.
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	The software constructs all or part of a command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended command when it is sent to a downstream component.
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	The software constructs all or part of an OS command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component.
CWE-88	Argument Injection or Modification	The software does not sufficiently delimit the arguments being passed to a component in another control sphere, allowing alternate arguments to be provided, leading to potentially security-relevant changes.

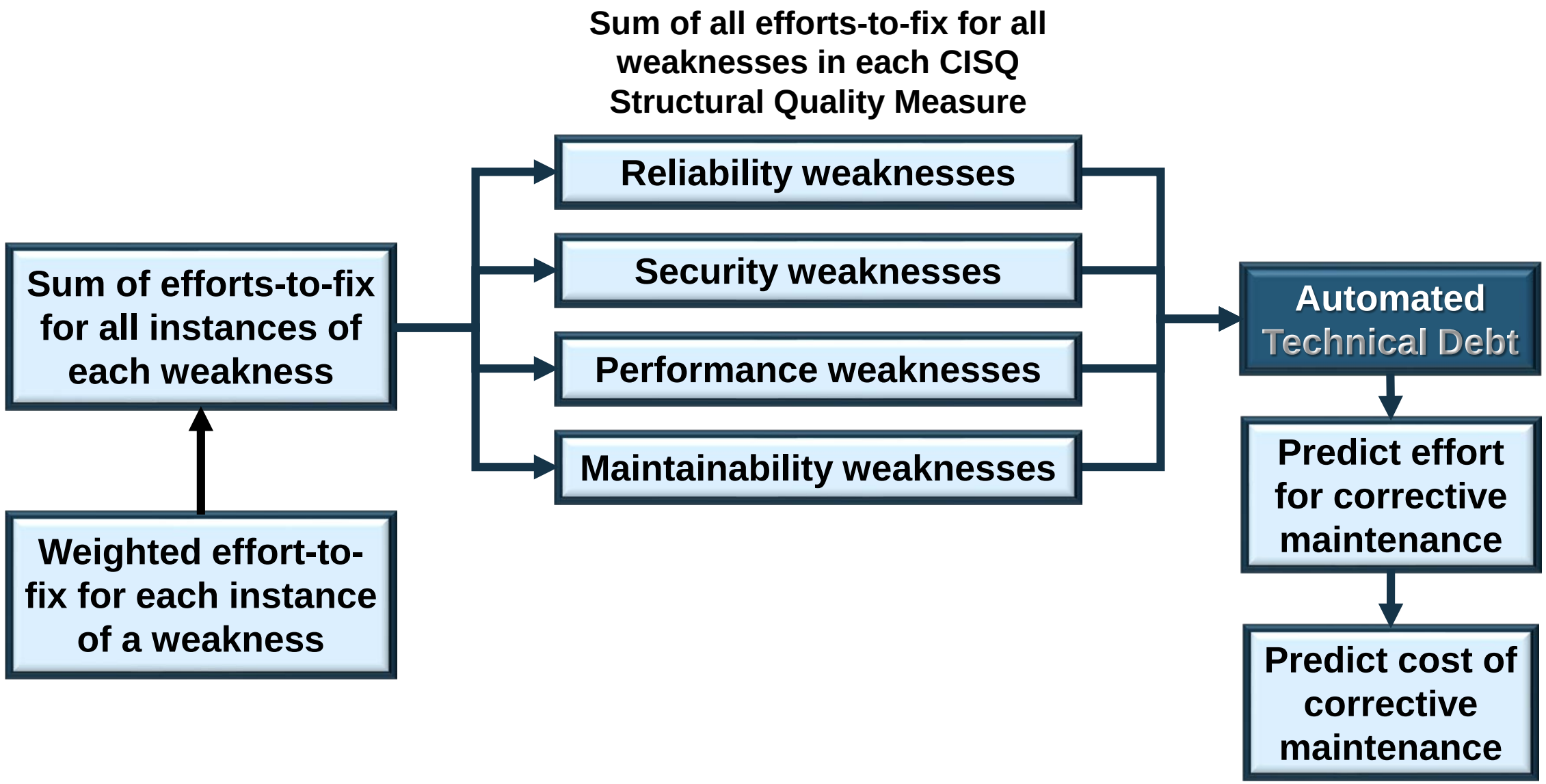
- **With all the functionality being embedded on chips, the line between embedded and IT software is blurring**
- **All CISQ weaknesses are now identified with CWE numbers**
- **Some CISQ weaknesses presented in parent-child relationships**
- **Attempting to get CISQ quality measures referenced in revision of ISO/IEC 25023**

Increases in the Number of CISQ Weaknesses

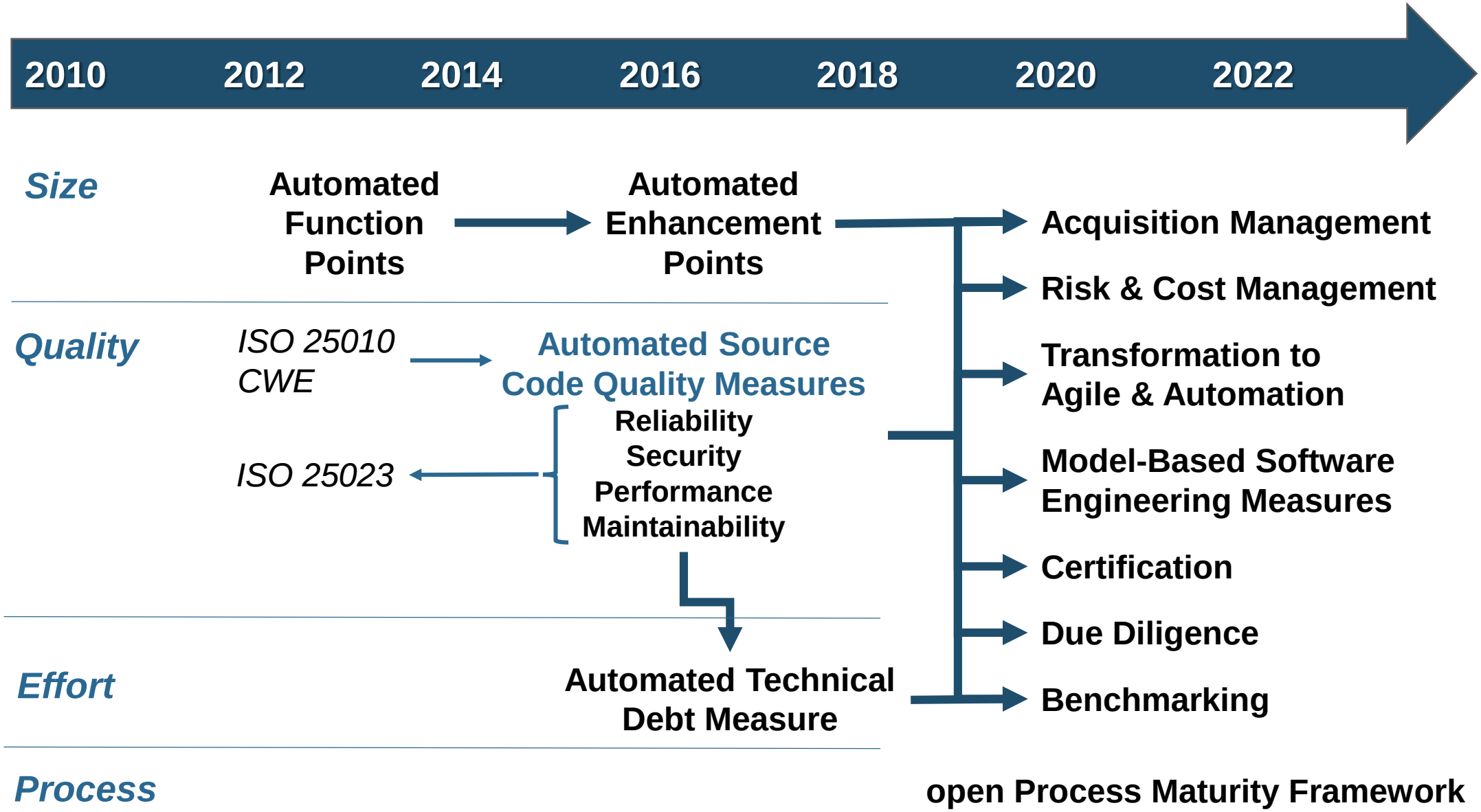
Embedded extensions

Quality Attribute	Parent weaknesses	Child weaknesses	Previous weaknesses
Reliability	36	38	29
Security	36	37	22
Performance	16	3	15
Maintainability	30	1	20
Totals	118	79	86

Automated Technical Debt Measure

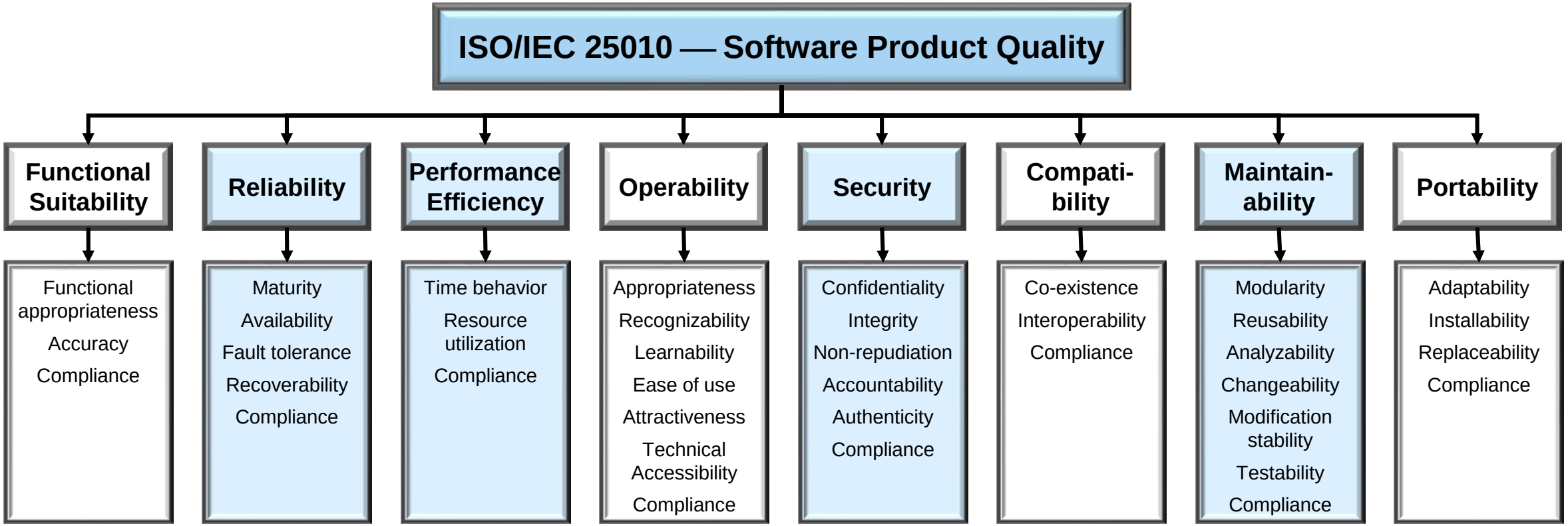


CISQ Roadmap



CISQ Conforms/Supplements ISO 25000 standards

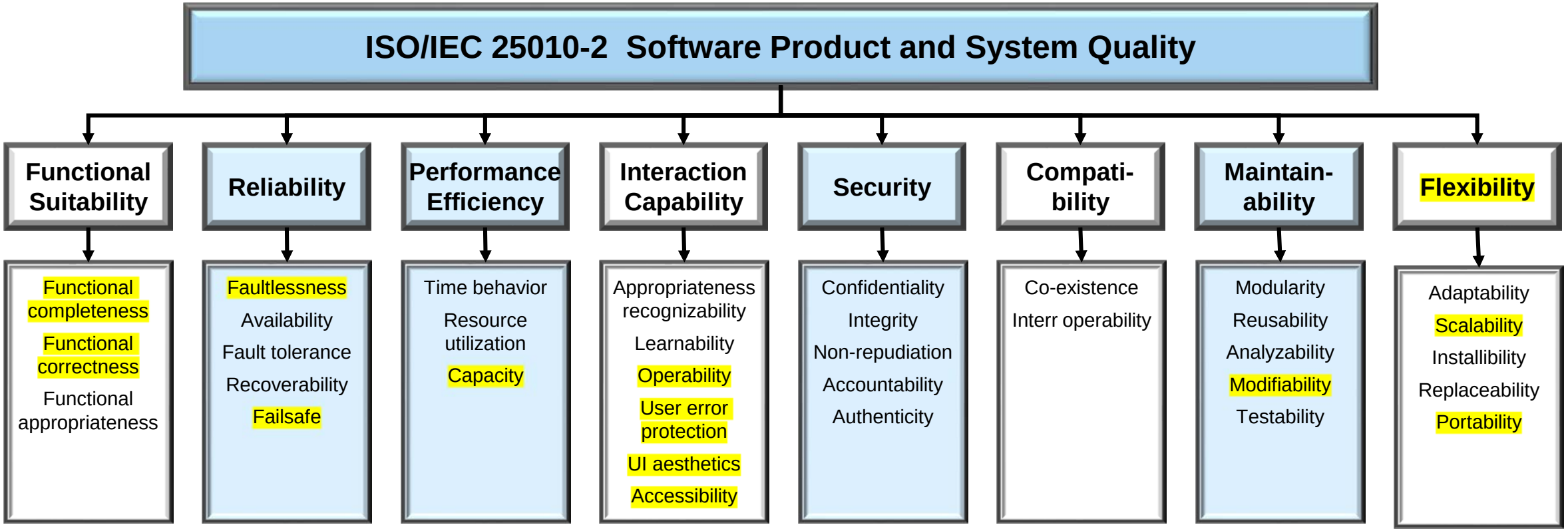
- **ISO/IEC 25010 defines a software product quality model of 8 quality characteristics**
- **CISQ conforms to ISO/IEC 25010 quality characteristic definitions**
- **ISO/IEC 25023 defines measures, but not automatable or at the source code level**
- **CISQ supplements ISO/IEC 25023 with automatable source code level measures**



CISQ automated structural quality measures are highlighted in blue

Revision of ISO/IEC 25010

- **ISO/IEC 25010 is being split into 3 parts – model overview, product quality, service quality**
- **Most changes are at sub-characteristic level (yellow), but one characteristic has changed**
- **US, UK, and India driving most changes, pressing for CISQ reference in ISO/IEC 25023**
- **Not final and can change – send feedback to curtis@acm.org**



CISQ automated structural quality measures are highlighted in blue

CISQ and the NIST Cybersecurity Framework

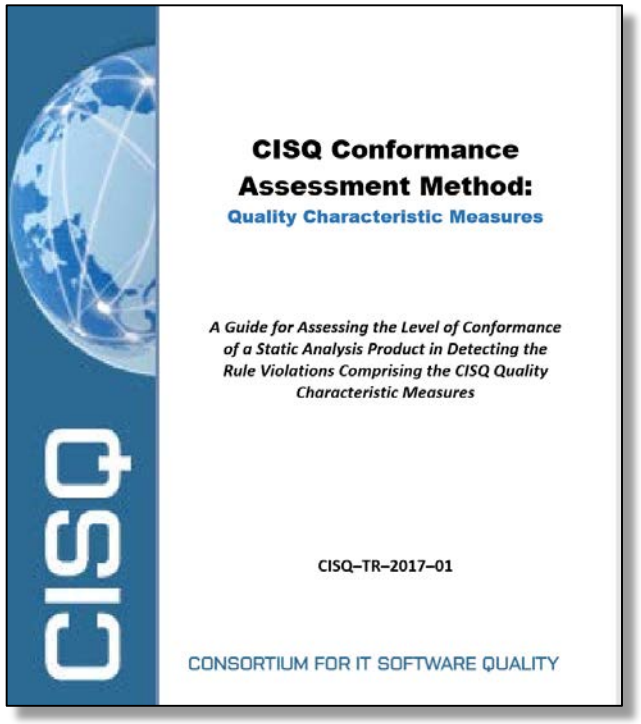
Consortium for IT Software Quality

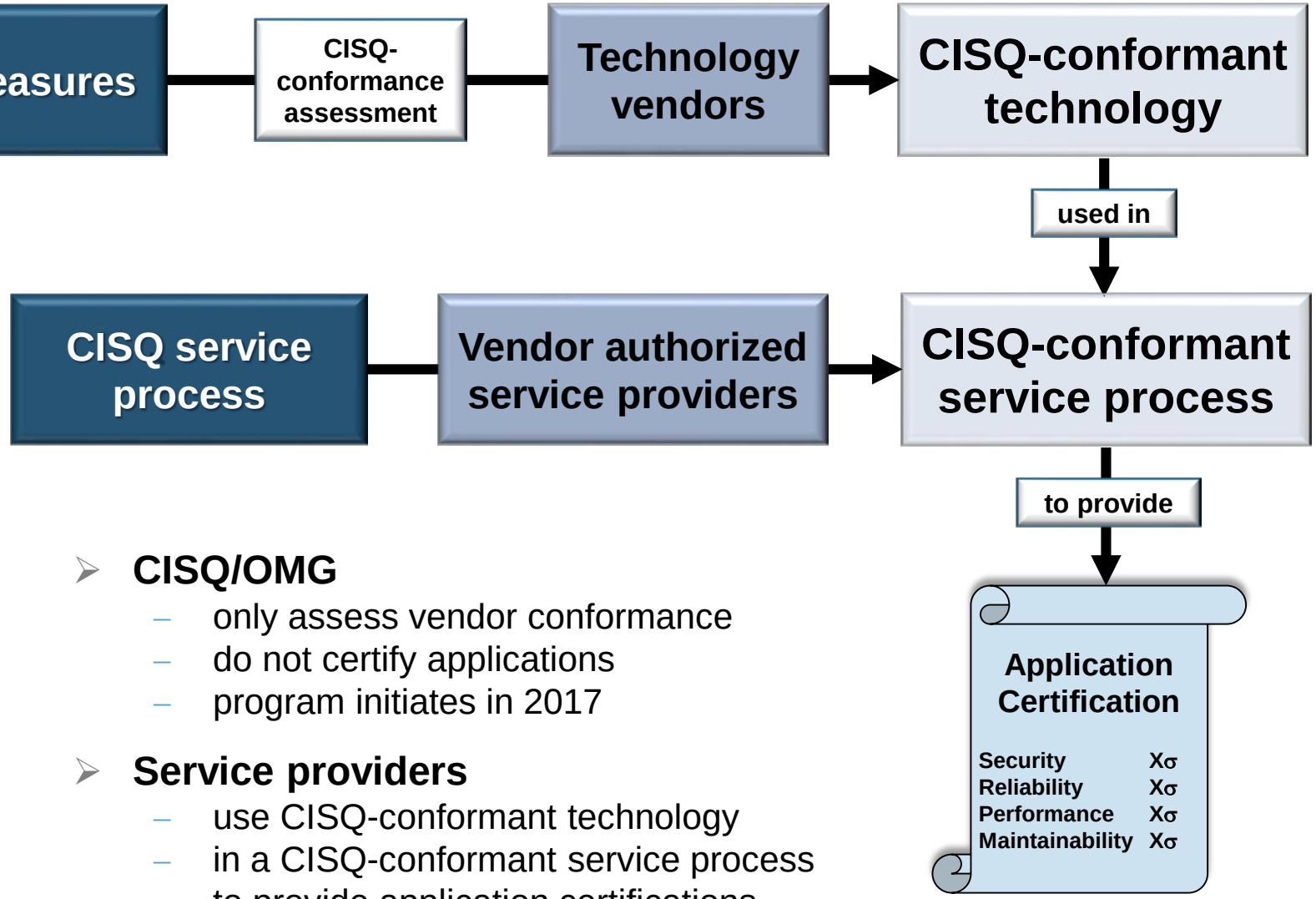
Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		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**

Application 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

Trustworthiness Measures for Model-Based Engineering

Objective — **Define quality measures based on counting severe architectural and design weaknesses that can be detected through analyzing formal models developed in Model-Based System Engineering (MBSE) languages and technologies.**

Two Focii —

1. **Quality of the architecture:**
   - **Architecture analysis might be the only way to find some weaknesses**
   - **Find other weaknesses earlier at the architectural level**
2. **Quality of the model of the architecture**

Sources —

1. **Architectural-level CWEs**
2. **Lists of architecture-level antipatterns**
3. **Vendor and system architect weakness lists or experiences**

What Is the open Process Maturity Framework?

Open Process Maturity Framework (oPMF):

- A meta-model for designing maturity models
- Develops organizations capable of sustaining improvement, change, agility, and innovation:
  - L2 Stabilize — *first, local work must be stable*
  - L3 Standardize — *economy of scale, foundation for lean*
  - L4 Optimize — *predictable, automated, reused, lean, etc.*
  - L5 Innovate — *continual experimentation & adaptation*
- Based on OMG's Business Process Maturity Model
- oPMF and maturity models derived from it are available for free on OMG and CISQ websites

Instantiations

Healthcare
Education
Engineering
Manufacturing
Retail
Government
Workforce
Etc.

Trustworthy Systems Manifesto

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 Membership Is Free — www.it-cisq.org

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