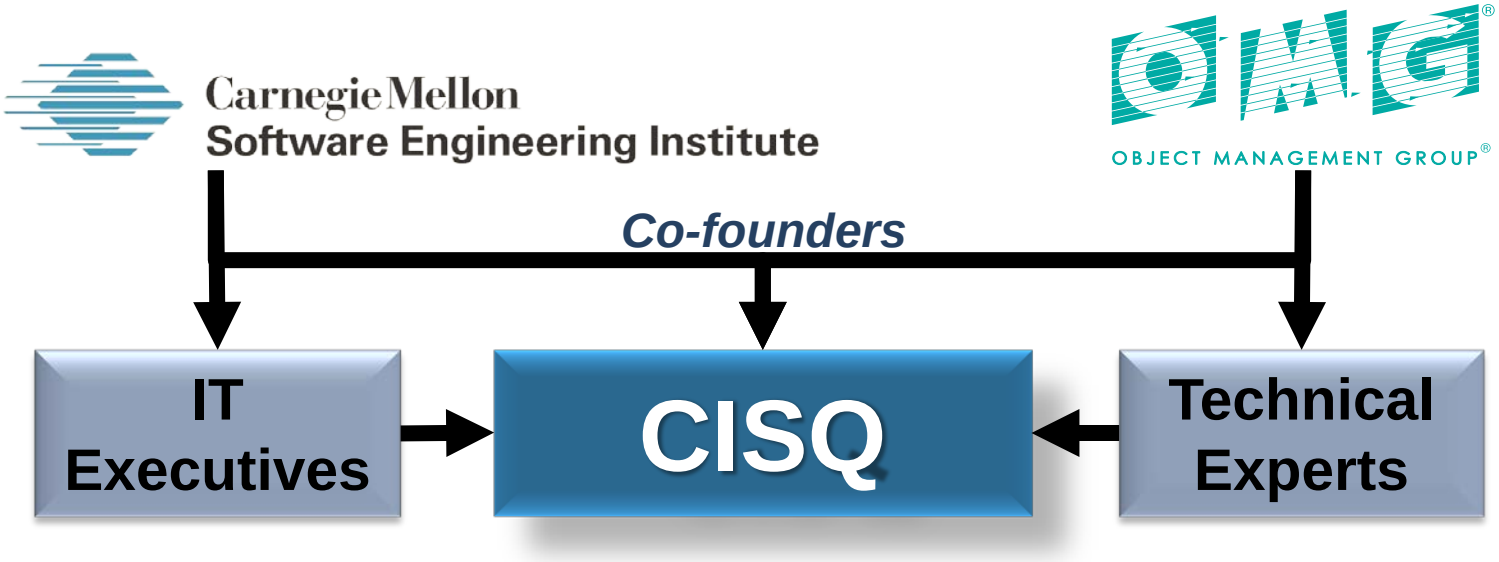
CISQ Standards for Measuring Software Risk, Security, and Technical Debt

Dr. Bill Curtis
Executive Director, CISQ

CISQ
Consortium for IT Software Quality

CISQ — 4th Generation Software Standards

Consortium for IT Software Quality



OMG Special Interest Group

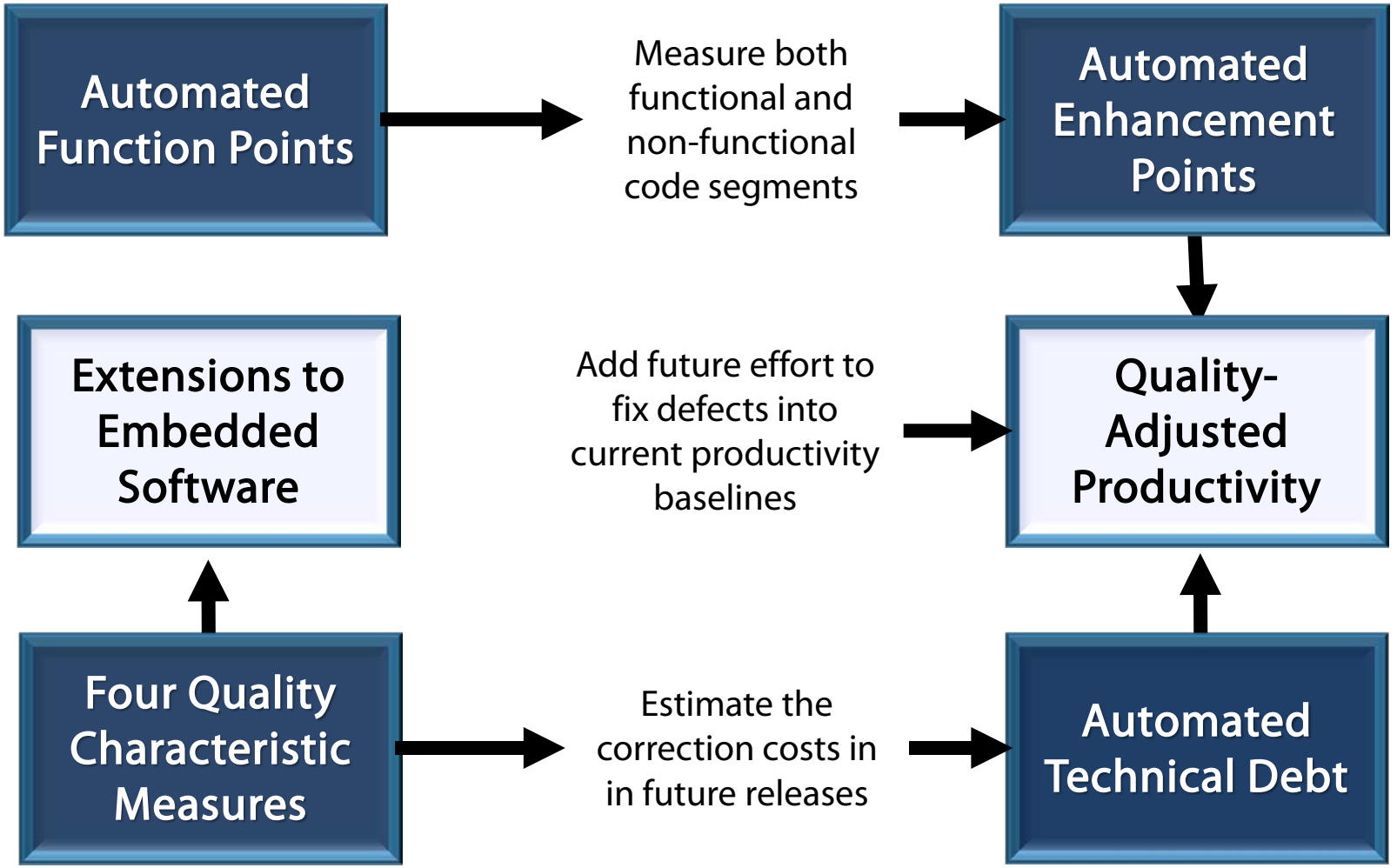
CISQ is chartered to define automatable measures of software size and quality that can be measured in the source code, and promote them to become Approved Specifications of the OMG®

CISQ Sponsors

SYNOPSYS® · Cognizant · SHPI · Tech Mahindra · CAST · CGI · NORTHROP GRUMMAN

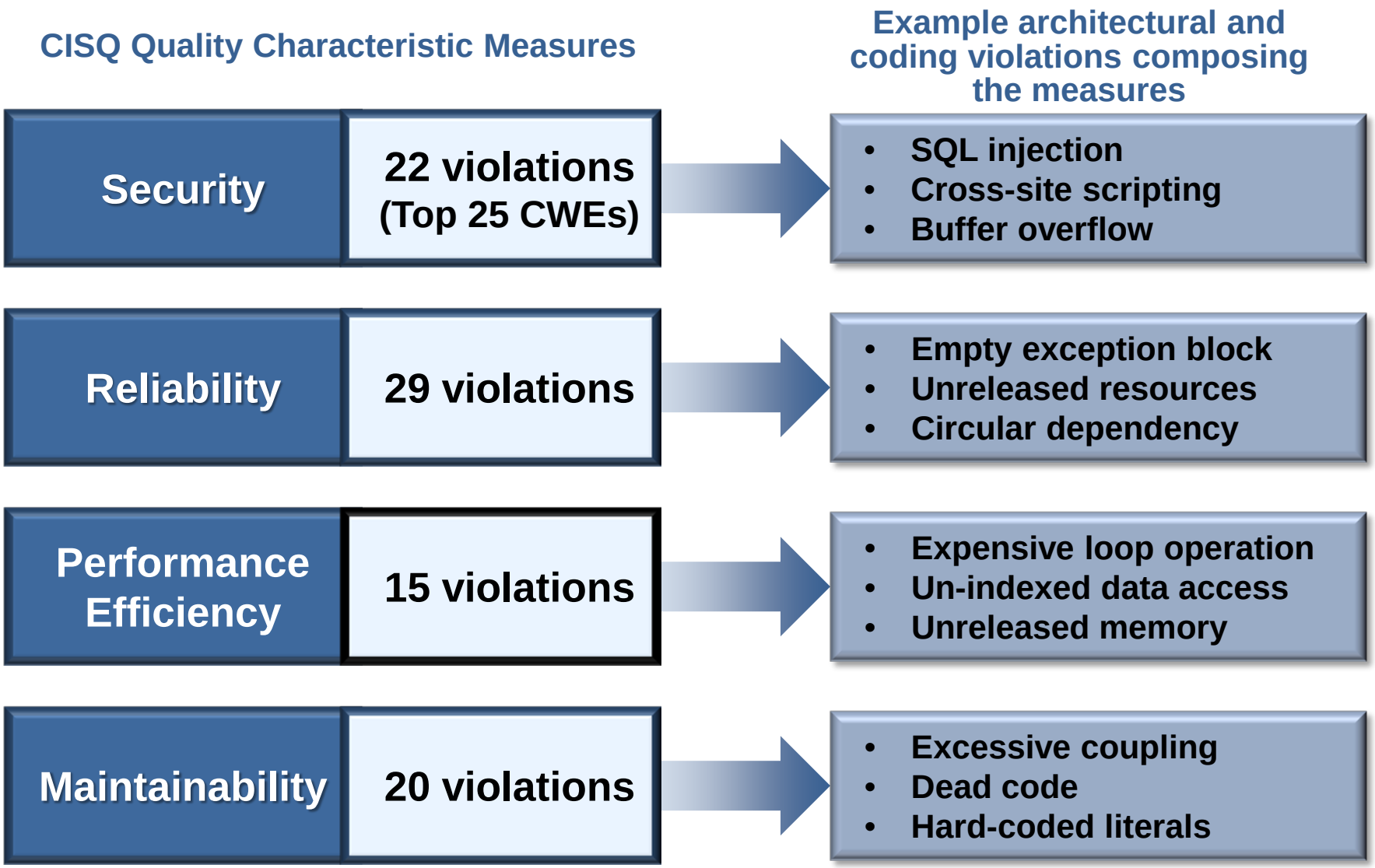
CISQ
Consortium for IT Software Quality

CISQ Measurement Standards Roadmap



CISQ Software Quality Measures

Consortium for IT Software Quality



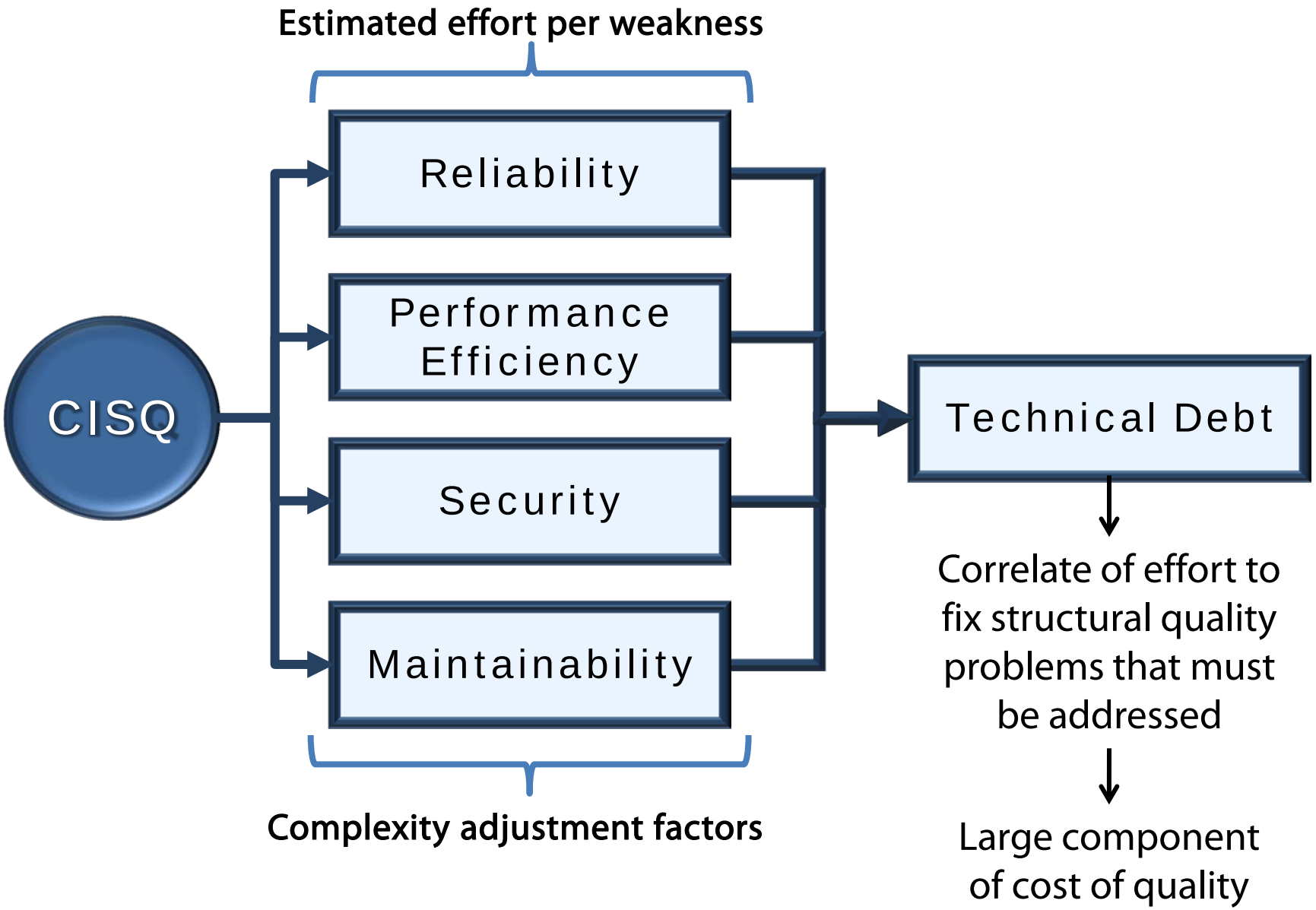
CISQ
Consortium for IT Software Quality

CISQ Embedded Extensions Project

1. Embedded software is becoming more like enterprise software
2. CISQ weaknesses are generally applicable to embedded software
3. Weaknesses can be organized in a parent-child relationship
4. Common Quality Enumeration needed to supplement CWEs

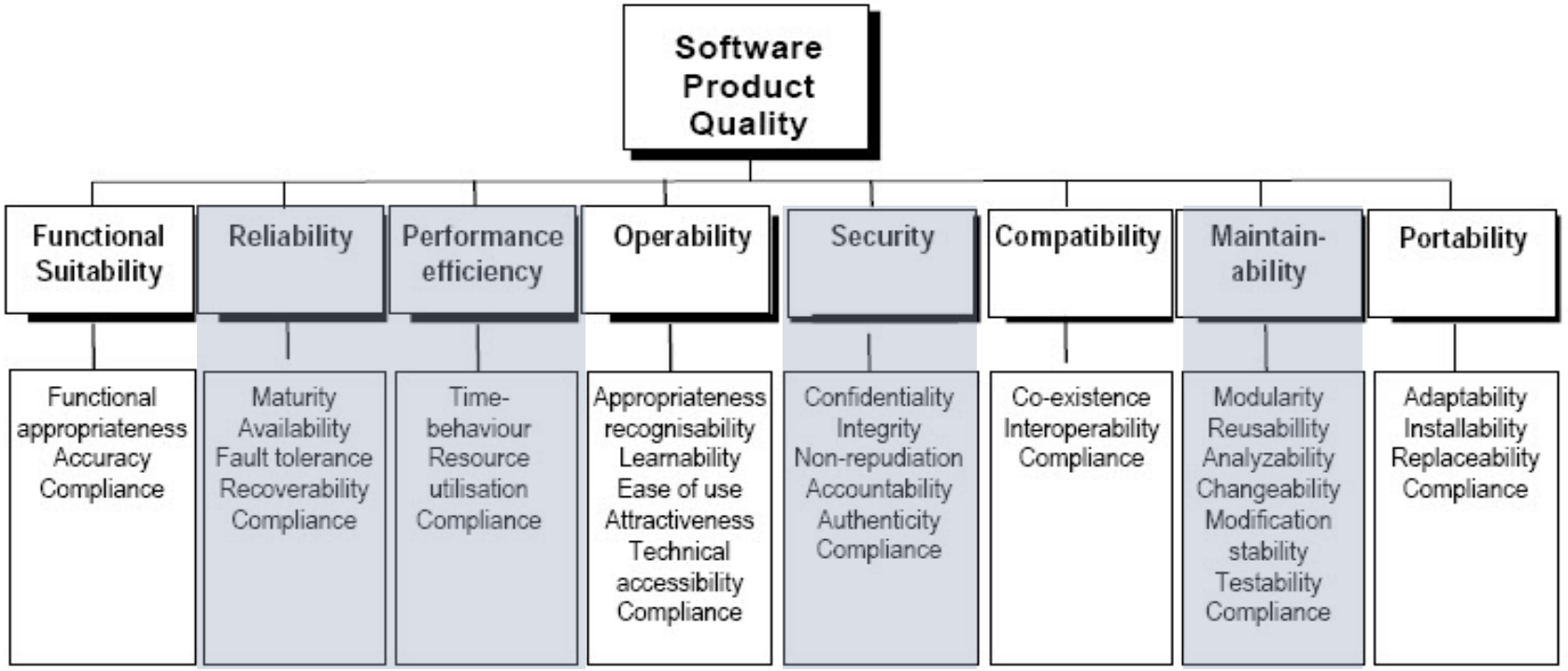
CISQ
Consortium for IT Software Quality

New — CISQ Technical Debt Measure



CISQ Measures and ISO 25000 Series

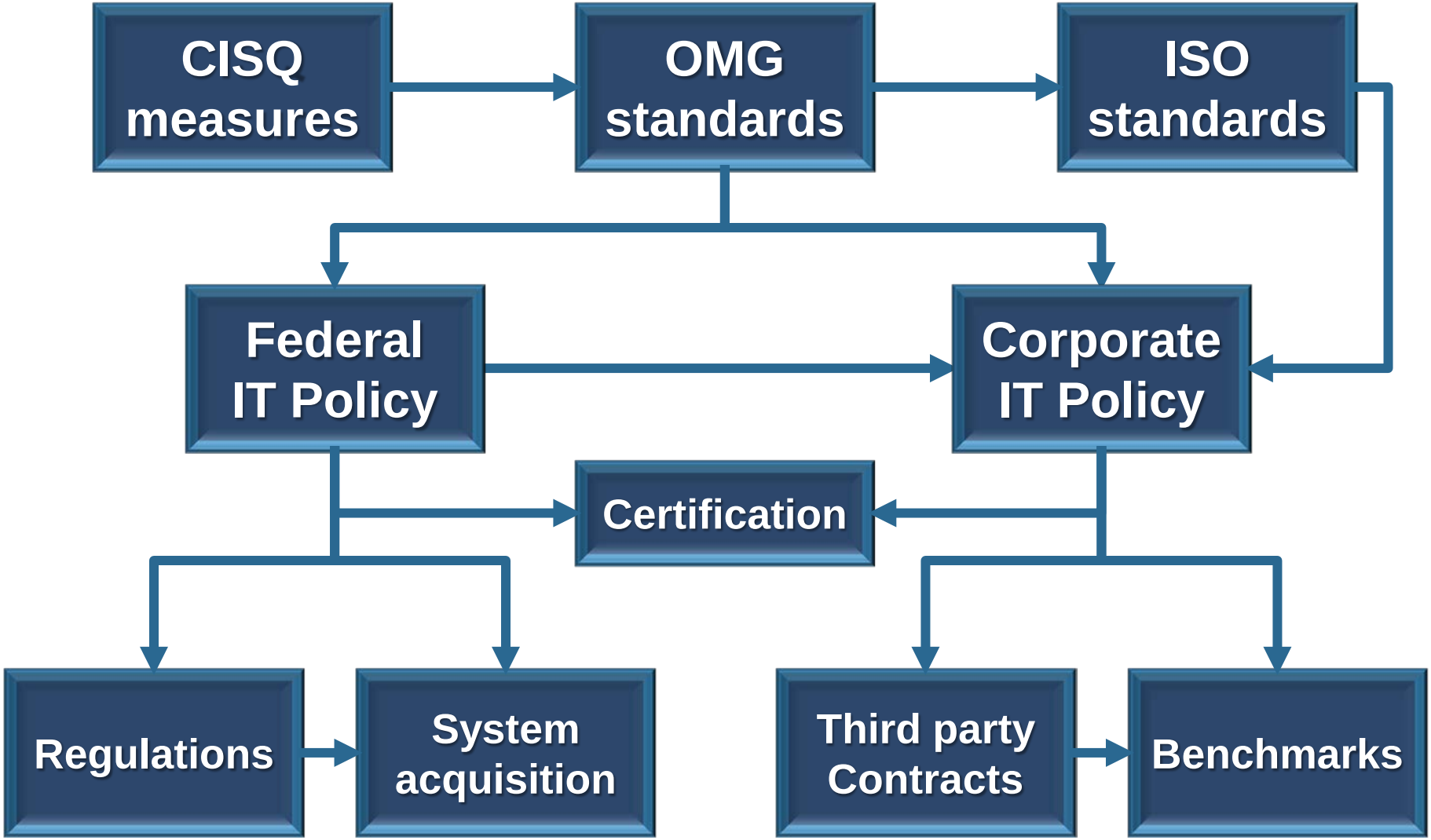
- **ISO 25010 defines quality characteristics and sub-characteristics**
- **CISQ conforms to ISO 25010 quality characteristic definitions**
- **ISO 25023 defines measures, but not at the source code level**
- **CISQ supplements ISO 25023 with source code level measures**



CISQ defined automatable measures for quality characteristics highlighted in blue

CISQ
Consortium for IT Software Quality

Deploying CISQ Measures

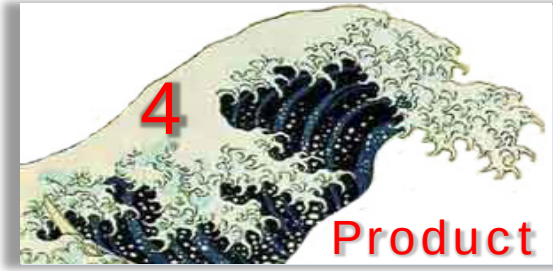


SEC Reg. SCI
Texas HB 8

US State Dept.
Gen. Serv. Admin.

CISQ
Consortium for IT Software Quality

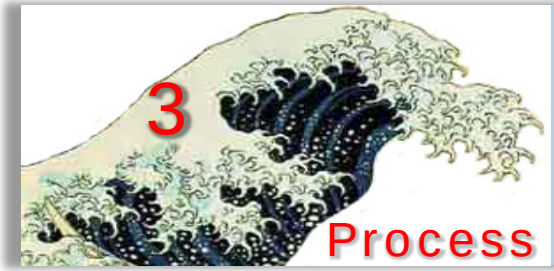
4th Wave in Software Engineering



What: Architecture, Structural measures, Reuse

When: 2002➔

Why: Improve engineering of software products



What: CMM, ITIL, PMBOK, Agile

When: 1990-2002

Why: Improve software management and discipline

What: Design methods, CASE tools

When: 1980-1990

Why: Give developers better aids to construct systems

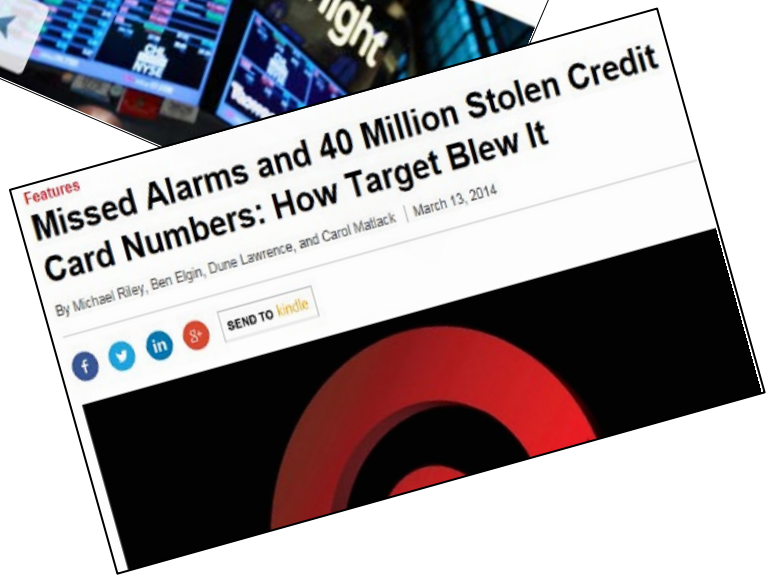
What: 3rd & 4th generation languages, structured programming

When: 1965-1980

Why: Give developers greater power for expressing programs

CISQ
Consortium for IT Software Quality

The Era of 9-Digit Defects



Executives, not development teams, are responsible for the liabilities of faulty software

They need a manifesto for dependable, trustworthy software

CISQ
Consortium for IT Software Quality

Challenges in the Agile Manifesto

Individuals and interactions over processes and tools

1. Occasionally becomes an excuse for undisciplined work
2. Agile methods are processes—shorter time scales require greater discipline
3. Agile and DevOps cannot be executed without tools chains
4. Agile focuses on teams (tribal) rather than on organizational capability

Working software over comprehensive documentation

1. Beware the temptation to short-circuit architecture and design
2. Bad architectures cannot be refactored

Customer collaboration over contract negotiation

1. Most often achieved when both are mature

Responding to change over following a plan

1. Control of commitments is critical for dependable, trustworthy software
2. Customers must own responsibility for controlling change

CISQ
Consortium for IT Software Quality

Example 'Assured Systems Manifesto'

As a greater portion of mission, business, and safety critical functionality is committed to software, we hold the following propositions as paramount:

1. Engineering discipline over individual craftsmanship
2. Adherence to evidence-tailored standards and methods
3. Automation to supplement human capabilities
4. Quality assurance to specified risk tolerance thresholds
5. Continuous detection and remediation of serious flaws
6. Etc.

Product focus is the core of the 4th generation software engineering

CISQ
Consortium for IT Software Quality

Join CISQ ! www.it-cisq.org