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

Dr. Bill Curtis
Executive Director, CISQ

CISQ
Consortium for IT Software Quality
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 Measurement Standards Roadmap

Automated Function Points

Measure both functional and non-functional code segments

Automated Enhancement Points

Add future effort to fix defects into current productivity baselines

Quality-Adjusted Productivity

Estimate the correction costs in future releases

Automated Technical Debt

Automated Function Points

Extensions to Embedded Software

Measure both functional and non-functional code segments

Automated Enhancement Points

Add future effort to fix defects into current productivity baselines

Quality-Adjusted Productivity

Estimate the correction costs in future releases

Automated Technical Debt

Four Quality Characteristic Measures

Measure both functional and non-functional code segments

Automated Enhancement Points

Add future effort to fix defects into current productivity baselines

Quality-Adjusted Productivity

Estimate the correction costs in future releases

Automated Technical Debt

Automated Function Points

Extensions to Embedded Software

Measure both functional and non-functional code segments

Automated Enhancement Points

Add future effort to fix defects into current productivity baselines

Quality-Adjusted Productivity

Estimate the correction costs in future releases

Automated Technical Debt

Four Quality Characteristic Measures
CISQ Quality Characteristic Measures

- **Security**: 22 violations (Top 25 CWEs)
- **Reliability**: 29 violations
- **Performance Efficiency**: 15 violations
- **Maintainability**: 20 violations

Example architectural and coding violations composing the measures:

- **Security**:
  - SQL injection
  - Cross-site scripting
  - Buffer overflow
- **Reliability**:
  - Empty exception block
  - Unreleased resources
  - Circular dependency
- **Performance Efficiency**:
  - Expensive loop operation
  - Un-indexed data access
  - Unreleased memory
- **Maintainability**:
  - Excessive coupling
  - Dead code
  - Hard-coded literals
Embedded software is becoming more like enterprise software

CISQ weaknesses are generally applicable to embedded software

Weaknesses can be organized in a parent-child relationship

Common Quality Enumeration needed to supplement CWEs
Technical Debt

Correlate of effort to fix structural quality problems that must be addressed

Estimated effort per weakness

Complexity adjustment factors

Reliability

Performance Efficiency

Security

Maintainability

Technical Debt

Large component of cost of quality
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 automutable measures for quality characteristics highlighted in blue
Deploying CISQ Measures

CISQ measures → OMG standards → ISO standards

Federal IT Policy → Certification → Corporate IT Policy

Certification → Regulations
- SEC Reg. SCI
- Texas HB 8

Certification → System acquisition
- US State Dept.
- Gen. Serv. Admin.

Certification → Third party Contracts
- Benchmarks
4th Wave in Software Engineering

1. **Language**
   - **What:** 3rd & 4th generation languages, structured programming
   - **When:** 1965-1980
   - **Why:** Give developers greater power for expressing programs

2. **Method**
   - **What:** Design methods, CASE tools
   - **When:** 1980-1990
   - **Why:** Give developers better aids to construct systems

3. **Process**
   - **What:** CMM, ITIL, PMBOK, Agile
   - **When:** 1990-2002
   - **Why:** Improve software management and discipline

4. **Product**
   - **What:** Architecture, Structural measures, Reuse
   - **When:** 2002
   - **Why:** Improve engineering of software products
Executives, not development teams, are responsible for the liabilities of faulty software. They need a manifesto for dependable, trustworthy software.
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
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

Product focus is the core of the 4th generation software engineering
Join CISQ! www.it-cisq.org

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.

Visit the Cyber Resilience Summit Knowledge Repository

CISQ Sponsors

CYBER RESILIENCE SUMMIT
Strategies to Modernize & Secure Government IT
MARCH 20, 2018 IN RESTON, VA U.S.A.

RSVP TODAY!