CISQ Quality Characteristic Measures
The Standards Are Here!

Dr. Bill Curtis
Executive Director, CISQ
What Is CISQ?

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
- Atos
- CAST
- Huawei
- Wipro

OMG Special Interest Group

Co-founders

IT Executives

CISQ

Technical experts
Why Measure IT Applications?

IT disasters now affect accountable for

- Board of Directors
- CEO, COO, CFO
- Business VPs
- Corporate Auditors
- CIO

- Governance
- Risk management
- Risk measurement
- Brand protection
- Customer experience

Evaluation of Application Quality with CISQ Measures
What Attributes Should Be Measured?

CISQ Quality Characteristic Measures

- **Security**: Ability to prevent unauthorized intrusions and data theft
  - Business outcomes: Damages, customer confidence

- **Reliability**: Ability to avoid outages and to recover operations quickly
  - Business outcomes: Damages, lost revenue, customer loss

- **Performance Efficiency**: Ability to avoid response degradation, resource overuse
  - Business outcomes: Lost customers, operating cost

- **Maintainability**: Ability to understand and modify software quickly
  - Business outcomes: Cost of ownership, time to market

http://it-cisq.org/standards/automated-quality-characteristic-measures

Automated Function Points

- An OMG Approved Specification
- Mirrors IFPUG counting guidelines, but automatable
- Specification developed by international team led by David Herron of David Consulting Group
- Growing commercial adoption
How Do CISQ Measures Relate 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

ISO/IEC 25010 Quality Characteristic Hierarchy

CISQ defined automatable measures for quality characteristics highlighted in blue
New Paradigm for Structural Measures

<table>
<thead>
<tr>
<th>Traditional metrics</th>
<th>measure program elements such as tokens, objects, or control structures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>These elements correlate with the potential for defects</td>
</tr>
<tr>
<td></td>
<td>These elements are defects</td>
</tr>
<tr>
<td>Violation measures</td>
<td>measure violations of good architectural and coding practice</td>
</tr>
<tr>
<td></td>
<td>Violations can be analyzed as patterns</td>
</tr>
</tbody>
</table>

CISQ Measures Violations

CISQ Quality Characteristic Measures

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Violations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>22 violations (Top 25 CWEs)</td>
</tr>
<tr>
<td>Reliability</td>
<td>29 violations</td>
</tr>
<tr>
<td>Performance Efficiency</td>
<td>15 violations</td>
</tr>
<tr>
<td>Maintainability</td>
<td>20 violations</td>
</tr>
</tbody>
</table>

Example architectural and coding violations composing the measures:

- SQL injection
- Cross-site scripting
- Buffer overflow
- Empty exception block
- Unreleased resources
- Circular dependency
- Expensive loop operation
- Un-indexed data access
- Unreleased memory
- Excessive coupling
- Dead code
- Hard-coded literals
CISQ Measures 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 Conformance and App Certification

- **CISQ measures**
  - CISQ-conformance assessment
  - Technology vendors
  - CISQ-conformant technology
  - used in
  - CISQ-conformant service process
  - to provide

- **CISQ service process**
  - CISQ-conformance assessment
  - Service providers
  - CISQ-conformant service process

- **CISQ/OMG**
  - only assess conformance
  - do not certify applications
  - program initiates 2016

- **Service providers**
  - use CISQ-conformant technology
  - in a CISQ-conformant service process
  - to provide application certifications

---

How Can CISQ Measures be Used?

Uses for measures:

1. Level of structural quality
2. Position on benchmark comparisons
3. Acceptable risk and cost thresholds

Business uses:

1. Due diligence and remedial priorities
2. Decisions on competitive investment
3. Probability of damaging events or costs

Certification Results

CRM rel. 3.2.1

Security XX
Reliability XX
Performance XX
Maintainability XX

To be supported when data are sufficient to set valid thresholds.
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 a computable metrics standard 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.

CISQ specifies how to measure four quality characteristics and Automated Function Points – both at the unit level and the whole system level.

ANY ORGANIZATION CAN MEASURE THEMSELVES AGAINST CISQ SPECIFICATIONS.

FIND OUT HOW

System Level

Unit Level

Software Characteristics

- RELIABILITY
- PERFORMANCE EFFICIENCY
- SECURITY
- MAINTAINABILITY
- FUNCTION POINTS