Advances in Software Quality Measurement

Dr. Bill Curtis
Executive Director

Why Measure IT Applications?

Six Digit Defects now affect accountable for

Board of Directors Governance
CEO, COO, CFO Risk management
Business VPs Risk measurement
Corporate Auditors Brand protection
CIO Customer experience

Evaluate Application Quality with CISQ Measures

© 2017. Consortium for IT Software Quality
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®.

OMG Special Interest Group

CISQ Co-founders
IT Executives

CISQ

Technical Experts

CISQ Sponsors

Reducing Operational Incidents & Costs

Study of structural quality measures and maintenance effort across 20 customers in a large global system integrator

Corrective Maintenance

TQI increase of .24 decreased corrective maintenance effort by 50%
CISQ/OMG Standards Process

OMG

Approved Measure Specifications

ISO Fasttrack

Deployment Workshops

CISQ Exec Forum

Automated Function Points

Reliability

Performance Efficiency

Security

Maintainability

OMG

Automated Function Points

• OMG Supported Specification for Automated Function Points

• Mirrors IFPUG counting guidelines, but automatable

• Specification developed by international team led by David Herron of David Consulting Group
Content of CISQ Measures

CISQ Quality Characteristic Measures | Example architectural and coding violations composing the CISQ measures
--- | ---
Security | 22 violations (Top 25 CWEs)
- SQL injection
- Cross-site scripting
- Buffer overflow

Reliability | 29 violations
- Empty exception block
- Unreleased resources
- Circular dependency

Performance Efficiency | 15 violations
- Expensive loop operation
- Un-indexed data access
- Unreleased memory

Maintainability | 20 violations
- Excessive coupling
- Dead code
- Hard-coded literals

The 22 CWEs in the Security Measure

- CWE-22 Path Traversal Improper Input Neutralization
- CWE-78 OS Command Injection Improper Input Neutralization
- CWE-79 Cross-site Scripting Improper Input Neutralization
- CWE-89 SQL Injection Improper Input Neutralization
- CWE-120 Buffer Copy without Checking Size of Input
- CWE-129 Array Index Improper Input Neutralization
- CWE-134 Format String Improper Input Neutralization
- CWE-252 Unchecked Return Parameter of Control Element Accessing Resource
- CWE-327 Broken or Risky Cryptographic Algorithm Usage
- CWE-396 Declaration of Catch for Generic Exception
- CWE-397 Declaration of Throws for Generic Exception
- CWE-434 File Upload Improper Input Neutralization
- CWE-456 Storable and Member Data Element Missing Initialization
- CWE-606 Unchecked Input for Loop Condition
- CWE-667 Shared Resource Improper Locking
- CWE-672 Expired or Released Resource Usage
- CWE-681 Numeric Types Incorrect Conversion
- CWE-706 Name or Reference Resolution Improper Input Neutralization
- CWE-772 Missing Release of Resource after Effective Lifetime
- CWE-789 Uncontrolled Memory Allocation
- CWE-798 Hard-Coded Credentials Usage for Remote Authentication
- CWE-835 Loop with Unreachable Exit Condition ('Infinite Loop')
Modern Apps Are a Technology Stack

- Architectural Compliance
- Transaction Risk
- Data Flow

Unit Level
- Code style & layout
- Expression complexity
- Class or program design
- Basic coding standards
- Developer level

Technology Level
- Single language/technology layer
- Intra-technology architecture
- Intra-layer dependencies
- Inter-program invocation
- Security vulnerabilities
- Development team level

System Level
- Integration quality
- Architectural compliance
- Risk propagation
- Resiliency checks
- Transaction integrity
- Function point
- Effort estimation
- Data access control
- SDK versioning
- Calibration across technologies
- IT organization level

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

CISQ automated quality characteristic measures highlighted in blue
CISQ in Service Level Agreements

Evaluate Product Quality against Targets in Quality Level Agreements

<table>
<thead>
<tr>
<th>Outsourcer</th>
<th>Automated Function</th>
<th>Reliability</th>
<th>Performance Efficiency</th>
<th>Security</th>
<th>Maintainability</th>
</tr>
</thead>
<tbody>
<tr>
<td>VENDOR 1</td>
<td>245</td>
<td>3.16</td>
<td>2.34</td>
<td>3.01</td>
<td>1.99</td>
</tr>
<tr>
<td>VENDOR 2</td>
<td>628</td>
<td>2.78</td>
<td>2.75</td>
<td>3.12</td>
<td>2.34</td>
</tr>
<tr>
<td>VENDOR 3</td>
<td>931</td>
<td>1.67</td>
<td>3.54</td>
<td>2.98</td>
<td>1.76</td>
</tr>
<tr>
<td>VENDOR 4</td>
<td>659</td>
<td>3.12</td>
<td>3.11</td>
<td>2.79</td>
<td>3.11</td>
</tr>
<tr>
<td>VENDOR 5</td>
<td>86</td>
<td>2.56</td>
<td>2.86</td>
<td>3.03</td>
<td>2.56</td>
</tr>
<tr>
<td>VENDOR 6</td>
<td>1047</td>
<td>3.76</td>
<td>2.89</td>
<td>2.97</td>
<td>2.55</td>
</tr>
</tbody>
</table>

Monitor and Manage Service Provider Performance

Emerging CISQ Measures

Automated Function Points
- Must measure functional and non-functional code segments

Automated Enhancement Points
- Must add future effort to fix bugs into productivity

Quality-Adjusted Productivity
- Must estimate the corrective costs in future releases

Automated Technical Debt
- Must measure the corrective costs in future releases

Extensions to Embedded Software
- Must add future effort to fix bugs into productivity
App Certification Using CISQ

CISQ measures
- CISQ-conformance assessment
- Technology vendors
- CISQ-conformant technology
  - used in
  - CISQ service process
  - Vendor authorized service providers
  - CISQ-conformant service process
  - to provide

- 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

Join CISQ!

www.it-cisq.org

ADVANCE THE MEASUREMENT OF SOFTWARE SIZE, QUALITY, AND RISK

- Become a sponsor to lend thought leadership
- Join CISQ to stay current