An Introduction to Automatable Standards for Software Measurement

Dr. Bill Curtis
Executive Director

CISQ
Consortium for IT Software Quality
In the Era of 9-Digit Defects...

Nine Digit Defects now affect Governor, Texas Legislature, DIR, Agency Heads, Agency CIOs, and are accountable for Governance, Risk management, Risk measurement, Taxpayer trust, and Customer UX. The need for measures of progress and quality is highlighted.

© 2018. Consortium for IT Software Quality
Modern Apps Are a Technology Stack

Unit Level
- Code style & layout
- Expression complexity
- Code documentation
- 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
- Application security
- Resiliency checks
- Transaction integrity
- Function point
- Effort estimation
- Data access control
- SDK versioning
- Calibration across technologies
- IT organization level
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/OMG Standards Process

- CISQ Exec Forum
  - Automated Function Points
  - Reliability
  - Performance Efficiency
  - Security
  - Maintainability
- OMG
  - Approved Measure Specifications
  - ISO Fasttrack
  - Deployment Workshops
• Mirrors IFPUG counting guidelines, but automatable

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

• Submitted thru OMG’s fasttrack as ISO 19515, currently under review
CISQ Quality Characteristic Measures

Example architectural and coding violations composing the CISQ 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

Security
- 22 violations (Top 25 CWEs)

Reliability
- 29 violations

Performance Efficiency
- 15 violations

Maintainability
- 20 violations
CISQ Conforms/Supplements 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

Software Product Quality

Functional Suitability
- Functional appropriateness
- Accuracy
- Compliance

Reliability
- Maturity
- Availability
- Fault tolerance
- Recoverability
- Compliance

Performance Efficiency
- Time behavior
- Resource utilization
- Compliance

Operability
- Appropriateness
- Recognizability
- Learnability
- Ease of use
- Attractiveness
- Technical Accessibility
- Compliance

Security
- Confidentiality
- Integrity
- Non-repudiation
- Accountability
- Authenticity
- Compliance

Compatibility
- Co-existence
- Interoperability
- Compliance

Maintainability
- Modularity
- Reusability
- Analyzability
- Changeability
- Modification stability
- Testability
- Compliance

Portability
- Adaptability
- Installability
- Replaceability
- Compliance

CISQ automated quality characteristic measures highlighted in blue
22 CWEs Form the CISQ 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')
Project adopts agile & DevOps

Significant gains in quality as team leverages code quality scans within each sprint.

Critical Findings

- Project is using static analysis on a limited basis realize 10% gains in quality
- Added, Modified, Deleted Function Points per Release

18 months 2 months 2 months 1 month 1 month
Improvement of Quality with Simultaneous Increase in Change

Initiate static analysis on Agile projects

Enterprise Agile Center of Excellence

Automated Function Points Added, Modified, Deleted

Q1 2015  Q2 2015  Q3 2015  Q4 2015  Q1 2016

Defects per Automated Function Point

AFP added, modified, deleted

Critical defects per AFP
CISQ Measures in System Acquisition

RFP: Include quality requirements and measures in project definition

SLA: Create quality targets using CISQ measures to set thresholds

SOW: Include software measurement and analysis as periodic project tasks

UAT: Measure against quality targets during acceptance testing
CISQ was referenced by the U.S. General Services Administration (GSA), in an Information Technology (IT) statement of work from the Office of the CIO in the Office of Public Buildings.

Page 21, section 5.9: Schedule 70 Blank Purchase Agreement for IT and Development Services...

“PB-ITS (Project Based IT Services) is seeking to establish code quality standards for its existing code base, as well as new development tasks. As an emerging standard, PB-ITS references the Consortium for IT Software Quality (CISQ) for guidance on how to measure, evaluate and improve software.”
### Sample Service Level ‘At Risk’ Matrix

**At Risk Amount and Allocation of Risk**

<table>
<thead>
<tr>
<th>Application Name</th>
<th>Tier 1 Metrics (Critical Service Levels)</th>
<th>At Risk Multiplier</th>
<th>Risk Allocation</th>
<th>At Risk Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>OMS</td>
<td>Security Findings 50%</td>
<td>30%</td>
<td>$15,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reliability Findings 30%</td>
<td></td>
<td>$9,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Application Pain Violations 20%</td>
<td></td>
<td>$6,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>100%</td>
<td>$30,000</td>
<td></td>
</tr>
<tr>
<td>CRM</td>
<td>Security Findings 30%</td>
<td>10%</td>
<td>$3,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reliability Findings 30%</td>
<td></td>
<td>$3,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Application Pain Violations 40%</td>
<td></td>
<td>$4,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>100%</td>
<td>$10,000</td>
<td></td>
</tr>
<tr>
<td>AMSS</td>
<td>Security Findings 50%</td>
<td>20%</td>
<td>$10,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reliability Findings 30%</td>
<td></td>
<td>$6,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Application Pain Violations 20%</td>
<td></td>
<td>$4,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>100%</td>
<td>$20,000</td>
<td></td>
</tr>
<tr>
<td>SDP</td>
<td>Security Findings 50%</td>
<td>20%</td>
<td>$10,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reliability Findings 30%</td>
<td></td>
<td>$6,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Application Pain Violations 20%</td>
<td></td>
<td>$4,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>100%</td>
<td>$20,000</td>
<td></td>
</tr>
<tr>
<td>Enabler</td>
<td>Security Findings 50%</td>
<td>20%</td>
<td>$10,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reliability Findings 30%</td>
<td></td>
<td>$6,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Application Pain Violations 20%</td>
<td></td>
<td>$4,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>100%</td>
<td>$20,000</td>
<td></td>
</tr>
</tbody>
</table>

**Total Billing Per Release:** $1,000,000

**Total At Risk Amount (10% of Bill):** $100,000

**Total Risk Pooler:** 100%

- Any time there is a default, the at-risk amount will be applied.
- Incentive is given to the at risk amount if Service Provider exceeds the Expected Service Level by 5% of the delta between the then current Expected and Perfection.
- Credits / Incentives are settled at the Annual Reset.

**Amount service provider has at risk in this Service Level is**

30% * 50% * $100K = $15,000
App Certification Using CISQ

- **CISQ measures**
  - CISQ-conformance assessment
  - Technology vendors
  - CISQ-conformant technology
  - 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

Application Certification

- Security $\times_\sigma$
- Reliability $\times_\sigma$
- Performance $\times_\sigma$
- Maintainability $\times_\sigma$
CISQ Home — 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.

Agenda is posted for Cyber Resilience Summit, October 19, Arlington, VA. Register today!

CISQ Sponsors

CGI
SYNOPSYS®
Booz Allen Hamilton
Cognizant

CYBER RESILIENCE SUMMIT
Modernizing and Securing Government IT
October 19, 2017
Army Navy Country Club
Arlington, VA U.S.A.