Measuring Software Risk with ISO 5055

Dr. Bill Curtis, Executive Director, Consortium for Information and Software Quality
The Era of the Nine-Digit Glitch

No person’s assets are safe while Wall Street is in session!
Density per KLOC of Security Weaknesses

Total sample
n = 994 Java apps
X̄ = 399.533 LOC
Max = 10,625,510 LOC
>1M LOC = 94 apps

Financial Services
n = 256
X̄ = 4.31 KLOC
Max = 38.97 KLOC

Curtis, et al. 2020 CRASH Report
What Is CISQ?

CISQ is chartered to specify measures of software size and quality that can be automated from source code, and promote them through OMG and other international standards organizations.
CISQ/OMG Quality Standards & ISO Fasttrack

OMG

- Reliability Measure
- Security Measure
- Maintainability Measure
- Performance Efficiency Measure
- Technical Debt Measure

ISO

- ISO/IEC 5055:2021
  - Automated Source Code Quality Measures
  - Data Protection Measure
  - Resource Sustainability Measure

© 2020 Consortium for Information and Software Quality (CISQ) www.it-cisq.org
ISO/IEC 25010 Support for Trustworthiness

ISO/IEC 25010
Software and System Product Quality Model

Functional Suitability
- Functional appropriateness
  - Accuracy

Reliability
- Maturity
  - Availability
  - Fault tolerance
  - Recoverability
- Time behavior
  - Resource utilization

Performance Efficiency
- Appropriateness
  - Recognizability
  - Learnability
- Ease of use
  - Attractiveness
  - Technical Accessibility

Usability
- Appropriate
  - Accountability
  - Transparency
  - Accountability

Security
- Confidentiality
  - Integrity
  - Non-repudiation
- Accountability
  - Authenticity
- Co-existence
  - Interoperability

Compatibility
- Modularity
  - Reusability
  - Analyzability
  - Changeability
- Modifiability
  - Stability
  - Testability

Maintainability
- Adaptability
  - Scalability
  - Installability
  - Portability
  - Replaceability

Flexibility
- Operational constraints
  - Risk identification
  - Failsafe
  - Hazard warning
  - Safe integration

Safety
- Operational constraints
  - Risk identification
  - Failsafe
  - Hazard warning
  - Safe integration
What Is ISO/IEC 5055:2021?

- Measures are calculated from automated detection and counting of weaknesses:
  - separate measure per quality factor
  - measures reportable as density, sigma level, compliance ratio, etc.

- Only weaknesses severe enough that they needed to be removed from the software

- 138 weaknesses selected by 75 experts from 26 companies in NA, EU, & Asia

- ISO 5055 includes:
  - list of weaknesses per measure
  - formal representation of weaknesses
  - detection patterns for weaknesses
Getting a Free ISO/IEC 5055:2021

You can pay 216 Swiss Francs for 5055 at https://www.iso.org/standard/80623....

.....or you can download it free from the Publicly Available Standard page
ISO 5055 Structural Quality Measures

ISO/IEC 5055:2021 Structural Quality Measures

Security
- 36 parent weaknesses
- 37 contributing weaknesses
- Example architectural and coding weaknesses:
  - SQL injection
  - Cross-site scripting
  - Buffer overflow

Reliability
- 35 parent weaknesses
- 39 contributing weaknesses
- Example architectural and coding weaknesses:
  - Improper synchronization
  - Improper error handling
  - Missing timeout

Performance Efficiency
- 16 parent weaknesses
- 3 contributing weaknesses
- Example architectural and coding weaknesses:
  - Costly loop operation
  - Un-indexed data access
  - Unreleased memory

Maintainability
- 29 parent weaknesses
- 0 contributing weaknesses
- Example architectural and coding weaknesses:
  - Excessive coupling
  - Hard-coded literals
  - Dead code

ISO/IEC 25010

© 2020 Consortium for Information and Software Quality (CISQ) www.it-cisq.org
Weakness Overlaps among Quality Factors

<table>
<thead>
<tr>
<th>Overlaps</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total overlaps</td>
<td>50</td>
</tr>
<tr>
<td>2 overlaps</td>
<td>44</td>
</tr>
<tr>
<td>3 overlaps</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Quality Factor Pairs</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security &amp; Reliability</td>
<td>42</td>
</tr>
<tr>
<td>Security &amp; Performance</td>
<td>6</td>
</tr>
<tr>
<td>Security &amp; Maintainability</td>
<td>4</td>
</tr>
<tr>
<td>Reliability &amp; Performance</td>
<td>5</td>
</tr>
<tr>
<td>Reliability &amp; Maintainability</td>
<td>6</td>
</tr>
</tbody>
</table>
Both Architectural and Coding Weaknesses

Multi-language, multi-layer architecture

- EJB
- PL/SQ
- Oracle SQL Server
- DB2
- T/SQL
- Hibernate
- Spring
- Struts
- .NET
- COBOL
- IMS
- Messaging
- Sybase

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

Technology Stack

1. Unit Level
   - Code size & 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

© 2020 Consortium for Information and Software Quality (CISQ) www.it-cisq.org
**ISO 5055 & the NIST Cybersecurity Framework**

ISO 5055 Security measure (and others) can be used in numerous processes of the NIST Cybersecurity Framework. Some examples:

- **Empirical software security risk tolerance thresholds**
- **Contractual SLAs and audits for software security**
- **Evaluation of software assets for security weaknesses**
- **Continual improvement of software security**
- **Periodic scans for software weaknesses**
- **Sharing software security and weakness data**
- **Security weaknesses are identified and mitigated**

ISO 5055 structural quality measures play an important requirements and verification role for ‘Build Security In’ approaches to cybersecurity.

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Unique Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>ID AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td>ID BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td>ID GV</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td>ID RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td>ID RM</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td></td>
<td>ID SC</td>
<td>Supply Chain Risk Management</td>
</tr>
<tr>
<td>Protect</td>
<td>PR AC</td>
<td>Identity Management and Access Control</td>
</tr>
<tr>
<td></td>
<td>PR AT</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td>PR DP</td>
<td>Information Protection Processes and Procedures</td>
</tr>
<tr>
<td></td>
<td>PR MA</td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td>PR PA</td>
<td>Protection Policy</td>
</tr>
<tr>
<td></td>
<td>PR AE</td>
<td>Audiences and Events</td>
</tr>
<tr>
<td></td>
<td>DE CM</td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td>Detect</td>
<td>DE AP</td>
<td>Detection Processes</td>
</tr>
<tr>
<td></td>
<td>DC CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td>DE AN</td>
<td>Analytics</td>
</tr>
<tr>
<td></td>
<td>RS MI</td>
<td>Mitigation</td>
</tr>
<tr>
<td>Respond</td>
<td>RS RP</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td>RS CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td>RS IM</td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td>RS DI</td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td>RS CO</td>
<td>Communications</td>
</tr>
</tbody>
</table>
Application Certification Using ISO 5055

- **ISO 5055 measures**
- **CISQ-conformance assessment**
- **Technology vendors**
- **5055-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 software

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

© 2020 Consortium for Information and Software Quality (CISQ) www.it-cisq.org
Developer Certification Using ISO 5055

- Dependable Developer Certification through OMG
- Test knowledge of ISO 5055 weaknesses
- Two types of questions – code snippets and text
- Need 300 participants for pilot testing
- Target availability in 2025

EXAMPLE TEXTUAL QUESTION:
Which of the following does not help thwart path traversal attacks?
1) Avoid reading files dynamically using user input
2) Validate/sanitize user input
3) Whitelist files whose contents can be included in responses to users
4) Require two-factor authentication for user access
5) Place user-accessible and non-accessible files on different servers
Calculating Technical Debt from ISO 5055

Sum of total efforts-to-fix for all weakness in each CISQ Quality Characteristic

- Reliability
- Security
- Performance
- Maintainability

Technical Debt

Predict effort for corrective maintenance

Predict cost of corrective maintenance

Sum of efforts-to-fix for all instances of each weakness

Weighted effort-to-fix for each instance of a weakness

CISQ is currently updating its Technical Debt standard to ISO 5055
Coming Attractions

2024 Cost of Poor Quality Software Report

SPDX 3.0
SBOM Standard

Flow Measures for Iterative and Agile
Visit CISQ at: www.it-cisq.org

- Approved CISQ/OMG standards
- Contract language
- Trustworthy Systems Manifesto
- Presentations
- Webinars
- Tutorials
- Whitepapers
- Use Cases
- Blogs
- News
- Current standards projects
- Process Maturity Metamodel
- Upcoming events
Become a CISQ Sponsor

Your sponsorship will fund the work that CISQ undertakes – giving your organization a leadership position to drive software standards, policy recommendations, software certifications, and activities to raise awareness of your organization’s support and commitment to software quality.

CISQ’s goals are to:

- Develop standards that automate software measurement
- Promote software security, reliability, and trustworthiness
- Share insight to software measurement best practices
- Deploy and train software quality standards and measures
- Influence software-related policies and regulations