CYBER RESILIENCE SUMMIT

From Securing the Supply Chain to Enterprise DevSecOps

October 13, 2020 – virtual meeting
Summit Moderators

Dr. Bill Curtis
Executive Director, CISQ

Luke McCormack
Cyber Resilience Summit Program Committee
CISQ/OMG Standards & ISO Fasttrack

OMG

Size

Automated Enhancement Points

Automated Function Points

Quality

Technical Debt Measure

Reliability Measure

Security Measure

Maintainability Measure

Performance Efficiency Measure

Automated Source Code Quality Measures

ISO

ISO/IEC 19515

Automated Function Points

Automated Source Code Quality Measures

Initial approval received

© 2020 Consortium for Information and Software Quality (CISQ) www.it-cisq.org
Automated Source Code Quality Measures

4 Quality Measures in ASCQM

<table>
<thead>
<tr>
<th>Quality Measure</th>
<th>Parent Weaknesses</th>
<th>Contributing Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>36</td>
<td>37</td>
</tr>
<tr>
<td>Reliability</td>
<td>35</td>
<td>39</td>
</tr>
<tr>
<td>Performance Efficiency</td>
<td>16</td>
<td>3</td>
</tr>
<tr>
<td>Maintainability</td>
<td>29</td>
<td>0</td>
</tr>
</tbody>
</table>

Example architectural and coding weaknesses included in the CISQ measures

- SQL injection
- Cross-site scripting
- Buffer overflow
- Improper synchronization
- Improper error handling
- Missing timeout
- Expensive loop operation
- Un-indexed data access
- Unreleased resource
- Excessive coupling
- Layer-skipping call
- Dead code

International team of experts selected the weaknesses included in CISQ measures

Measures selected for severity of impact on operational problems or cost of ownership

Measures include both IT and embedded system weaknesses

Large percent of weaknesses include architectural flaws

All CISQ Weaknesses are CWEs
CISQ Supplements ISO/IEC 25000 Standards

- ISO/IEC 25010 defines a software product quality model of 8 quality characteristics
- CISQ conforms to ISO/IEC 25010 quality characteristic definitions
- ISO/IEC 25023 defines measures, but not automatable or at the source code level
- CISQ supplements ISO/IEC 25023 with automatable source code level measures

ISO/IEC 25010 — 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 structural quality measures are highlighted in blue
Deploying CISQ Measures in Public Sector

CISQ measures → OMG standards → ISO standards → Public IT Policy → Corporate IT Policy → Third party Contracts → Benchmarks

- Regulations: Sec. & Exch. Com., State of Texas
CISQ Membership Is Free — www.it-cisq.org

Over 3,000 individual members from large software-intensive organizations:

- Accenture
- AT&T
- Amazon
- Infosys
- Bosch
- Booz Allen Hamilton
- CREDIT SUISSE
- IAOP
- Allianz
- Gartner
- Capgemini
- Citi
- Capital One
- Dell
- FedEx
- Discovery Health
- CenturyLink
- MITRE
- Barclays

© 2020 Consortium for Information and Software Quality (CISQ) www.it-cisq.org
THANK YOU FOUNDERS & SPONSORS