How Can VMOs Ensure Vendor-Supplied Software is Trustworthy?

IAOP Webinar
February 6, 2019

Dr. Bill Curtis
Executive Director, CISQ

International Standards for Automating Software Size and Structural Quality Measurement
75% Of vendors’ developers have less than 3 years experience

10x Difference between experienced and novice developer

$25↑ Hourly rate card of outsourced developers continually rises

30+% Annual turnover creates constant learning curve destroying benefits of labor arbitrage

Sources: The Economics of Software Quality, Jones, Bonsignour; CAST Research Labs
The Shift to Outcome-based Contracting

Projected business value

LOWEST BUSINESS VALUE
HIGHEST COST PRESSURE

Input-based contract
- Time & materials
- Fixed capacity
- Low incentive

Output-based contract
- Size (Function Points)
- Incidents, Tickets
- Velocity, Delivery rate
- Quality, Delivered defects

Outcome-based contract
- Service delivered
- Impact on business
- Satisfaction

HIGHEST BUSINESS VALUE
LOWEST COST PRESSURE

OUTCOME-BASED CONTRACTS ARE GROWING RAPIDLY

Deloitte. of CIOs and CTOs find outcome-based contracts most effective

Source: Deloitte 2014 Global Outsourcing and Insourcing Survey

© 2019 Consortium for IT Software Quality (CISQ) www.it-cisq.org
## ISG Predictions on Engagement Models

**Source:** ISG December 2016 *The Three Waves in the Evolution of the Engineering Services Outsourcing Industry*

<table>
<thead>
<tr>
<th>Delivery Model</th>
<th>2015</th>
<th>2020</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Offshore: 80%</td>
<td>Offshore: 60%</td>
</tr>
<tr>
<td></td>
<td>Onsite: 20%</td>
<td>Onsite, Nearshore: 40%</td>
</tr>
</tbody>
</table>

**Table:**

<table>
<thead>
<tr>
<th></th>
<th>2015</th>
<th>2020</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Delivery Model</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Offshore: 80%</td>
<td></td>
<td>Offshore: 60%</td>
</tr>
<tr>
<td>Onsite: 20%</td>
<td></td>
<td>Onsite, Nearshore: 40%</td>
</tr>
</tbody>
</table>
From Process to Product Measurement

Process focus

Contributes to, but does not measure or guarantee product quality

Product focus

Must be supplemented by software product measurement before and during acceptance

CISQ Measures assess the structural quality of the delivered software product
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 Structural Quality Measures

#### Security
- **22 weaknesses**
- (Top 25 CWEs)
  - SQL injection
  - Cross-site scripting
  - Buffer overflow

#### Reliability
- **29 weaknesses**
  - Empty exception block
  - Unreleased resources
  - Circular dependency

#### Performance Efficiency
- **15 weaknesses**
  - Expensive loop operation
  - Un-indexed data access
  - Unreleased memory

#### Maintainability
- **20 weaknesses**
  - Excessive coupling
  - Dead code
  - Hard-coded literals

---

An international team of experts selected the weaknesses to include in CISQ measures based on the severity of their impact on operational problems or cost.

Only weaknesses considered severe enough that they must be remediated were included in the CISQ measures.

CISQ Structural Quality measures are currently being extended to embedded systems software.

CISQ measures conform to quality characteristic definitions in ISO/IEC 25010 and supplement measures in ISO/IEC 25023.
Six Ways to Engage Vendors with CISQ Measures

**Recommendation**
- Contact vendor delivery leaders to suggest they use CISQ measures for all ADM work

**RFP**
- Initial statement of requirements and project definition can list CISQ measures for assessing software quality

**Scorecard**
- Measurement and discussion in governance committees to ensure SLAs & KPIs are met

**SOW**
- Definition of specific project scope and deliverables can include specification of quality measures

**SLAs**
- Treat software enhancements and maintenance as a service; track levels, penalties, credits

**Acceptance criteria**
- Demand minimal set of measurable acceptance criteria for any new development or release
Deploying a vendor measurement program is a process, not a big bang event.

- **Start**
  - Roll out CISQ measurement

- **6 months**
  - Collect initial set of metrics
  - Socialize metrics with vendors

- **6-12 months**
  - Roll out scorecard program
  - Include scorecards in management meetings with vendors
  - Introduce service levels into MSAs
  - Select key applications for SLAs
  - Use internal baselines for project acceptance criteria
  - Continually evaluate and update baselines
CISQ has been referenced by the U.S. General Services Administration (GSA), formally citing CISQ requirements in a Information Technology (IT) statement of work from the Office of the CIO for the Office of Public Buildings. GSA is an independent agency of the U.S. government that supports general services of Federal agencies.

See page 21, section 5.9 in GSA’s document, 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 Scorecard

Scorecard Service Providers

<table>
<thead>
<tr>
<th>VENDOR</th>
<th>Reliability</th>
<th>Performance Efficiency</th>
<th>Security</th>
<th>Maintainability</th>
</tr>
</thead>
<tbody>
<tr>
<td>VENDOR 1</td>
<td>3.16</td>
<td>2.34</td>
<td>3.01</td>
<td>1.99</td>
</tr>
<tr>
<td>VENDOR 2</td>
<td>2.78</td>
<td>3.38</td>
<td>3.12</td>
<td>2.34</td>
</tr>
<tr>
<td>VENDOR 3</td>
<td>1.67</td>
<td>3.54</td>
<td>2.98</td>
<td>1.76</td>
</tr>
<tr>
<td>VENDOR 4</td>
<td>3.12</td>
<td>3.11</td>
<td>2.79</td>
<td>3.11</td>
</tr>
<tr>
<td>VENDOR 5</td>
<td>3.56</td>
<td>3.88</td>
<td>3.03</td>
<td>3.42</td>
</tr>
<tr>
<td>VENDOR 6</td>
<td>3.76</td>
<td>2.89</td>
<td>2.97</td>
<td>2.55</td>
</tr>
</tbody>
</table>

Scores based on a 1 to 4 quality rating system

Monitor Performance Over Time

Scores based on a 1 to 4 quality rating system
### At Risk Amount and Allocation of Risk

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

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

**Total Risk Pooler:** 100%

<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><strong>OMS</strong></td>
<td>Security Findings</td>
<td>50%</td>
<td>30%</td>
<td>$15,000</td>
</tr>
<tr>
<td></td>
<td>Reliability Findings</td>
<td>30%</td>
<td></td>
<td>$9,000</td>
</tr>
<tr>
<td></td>
<td>Application Pain Violations</td>
<td>20%</td>
<td></td>
<td>$6,000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100%</td>
<td></td>
<td>$30,000</td>
</tr>
<tr>
<td><strong>CRM</strong></td>
<td>Security Findings</td>
<td>30%</td>
<td>10%</td>
<td>$3,000</td>
</tr>
<tr>
<td></td>
<td>Reliability Findings</td>
<td>30%</td>
<td></td>
<td>$3,000</td>
</tr>
<tr>
<td></td>
<td>Application Pain Violations</td>
<td>40%</td>
<td></td>
<td>$4,000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100%</td>
<td></td>
<td>$10,000</td>
</tr>
<tr>
<td><strong>AMSS</strong></td>
<td>Security Findings</td>
<td>50%</td>
<td>20%</td>
<td>$10,000</td>
</tr>
<tr>
<td></td>
<td>Reliability Findings</td>
<td>30%</td>
<td></td>
<td>$6,000</td>
</tr>
<tr>
<td></td>
<td>Application Pain Violations</td>
<td>20%</td>
<td></td>
<td>$4,000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100%</td>
<td></td>
<td>$20,000</td>
</tr>
<tr>
<td><strong>SDP</strong></td>
<td>Security Findings</td>
<td>50%</td>
<td>20%</td>
<td>$10,000</td>
</tr>
<tr>
<td></td>
<td>Reliability Findings</td>
<td>30%</td>
<td></td>
<td>$6,000</td>
</tr>
<tr>
<td></td>
<td>Application Pain Violations</td>
<td>20%</td>
<td></td>
<td>$4,000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100%</td>
<td></td>
<td>$20,000</td>
</tr>
</tbody>
</table>

- **OMS** example:
  - 30% * 50% * $100K = $15,000

- **Any time there is a default, the at-risk amount will be forfeited.**
- **Credits / Incentives are settled at the Annual Reset.**

10% is for example.
Application Certification Using CISQ Measures

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

- **CISQ service process**
  - Vendor authorized service providers
  - CISQ-conformant service process

- **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 $X_\sigma$
  - Reliability $X_\sigma$
  - Performance $X_\sigma$
  - Maintainability $X_\sigma$
Vendor Management Resources

Website area for Vendor Management use case
• http://it-cisq.org/vendor-management/

Whitepaper about the concept of using CISQ metrics in SLAs

Whitepaper with detailed step-by-step instructions for putting CISQ metrics in SLAs

Sample acceptance criteria using CISQ metrics

Sample RFP from U.S. General Services Administration (GSA) that uses CISQ as part of it’s requirement for quality software
• Go to section 5.9, page 21 of 73
As a greater portion of mission, business, and safety critical functionality is committed to software-intensive systems, these systems become one of, if not the largest source of risk to enterprises and their customers. Since corporate executives are ultimately responsible for managing this risk, we establish the following principles to govern software-system development and deployment.

1. Engineering discipline in product and process
2. Quality assurance to risk tolerance thresholds
3. Traceable properties of system components
4. Proactive defense of the system and its data
5. Resilient and safe operations
CISQ Membership Is Free — www.it-cisq.org

Over 2000 individual members from large software-intensive organizations:

Member → CISQ Members Area
Sponsor → CISQ Events

CISQ Sponsors

iTrustworthy Systems Manifesto

5 principles to govern system development and deployment:
1. Engineering discipline in product and process
2. Quality assurance to risk tolerance thresholds
3. Traceable properties of system components
4. Proactive defense of the system and its data
5. Resilient and safe operations
Questions