REDUCING IT RISK WITH SUPPLIERS BY REDUCING ARCHITECTURAL AND TECHNICAL DEBT

Dave Norton
Executive Director
Consortium for Information & Software Quality
david.norton@it-cisq.org
Two Basic Truths

Things are more complex and the pace of change is relentless
Finance Cyber Incidents in the UK, Up 1087% Increase Year on Year

- 21%, are related to third-party failure, i.e., systems the reporting organization did not control.
- However, many of the other incidents had their origins in third-party developed software now owned by the reporting organization.

<table>
<thead>
<tr>
<th>Root Cause</th>
<th>2019</th>
<th>2018</th>
<th>% of Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware and software issues</td>
<td>157</td>
<td>64</td>
<td>19%</td>
</tr>
<tr>
<td>Change management</td>
<td>146</td>
<td>53</td>
<td>18%</td>
</tr>
<tr>
<td>Third-party failure</td>
<td>174</td>
<td>79</td>
<td>21%</td>
</tr>
<tr>
<td>Cyber-attack - Distributed denial of service (DDoS)</td>
<td>10</td>
<td>2</td>
<td>1%</td>
</tr>
<tr>
<td>Cyber-attack - Malware</td>
<td>16</td>
<td>5</td>
<td>2%</td>
</tr>
<tr>
<td>Cyber-attack - Ransomware</td>
<td>19</td>
<td>0</td>
<td>2%</td>
</tr>
<tr>
<td>Cyber-attack - Phishing or other compromise of credentials</td>
<td>48</td>
<td>29</td>
<td>6%</td>
</tr>
<tr>
<td>To be confirmed</td>
<td>93</td>
<td>82</td>
<td>11%</td>
</tr>
<tr>
<td>Human error</td>
<td>47</td>
<td>24</td>
<td>6%</td>
</tr>
<tr>
<td>Process/control failure</td>
<td>45</td>
<td>17</td>
<td>5%</td>
</tr>
<tr>
<td>Failure to manage adequate IT capacity</td>
<td>25</td>
<td>4</td>
<td>3%</td>
</tr>
<tr>
<td>External factors</td>
<td>17</td>
<td>3</td>
<td>2%</td>
</tr>
<tr>
<td>Theft</td>
<td>11</td>
<td>3</td>
<td>1%</td>
</tr>
<tr>
<td>Cause unknown</td>
<td>11</td>
<td>5</td>
<td>1%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>819</strong></td>
<td><strong>370</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>
Total Cost Of Ownership Is On The Rise

Between 84% to 92% of the total cost of a system is operating expense (opex), so why is all the focus on the 8% to 16% initial capital expense (capex)
**Technical debt** is a concept in software development that reflects the implied cost of additional rework caused by choosing an easy (limited) solution now instead of using a better approach that would take longer.
The Suppliers Have To Build Quality In From The Start
The Suppliers Have To Build Quality In From The Start
Self-Regulation Is Failing, and The Pressure Is Building In The Boardroom.

Angry Citizen, Markets & Business ➔ Lead To Concerned Politicians ➔ Regulators Forced To Act ➔ Recrimination In The Boardroom

CEO  COO  CIO  CFO  CCO
The Nine-Digit Glitch

Nine Digit Defects

Now affect
- Board of Directors
- CEO, COO, CFO
- Business VPs
- Corporate Auditors
- CIO

Accountable for
- Governance
- Risk management
- Business Continuity
- Brand protection
- Customer experience
CEOs Are Paying The Price For Poor IT Quality

“British Airways’ chief executive Álex Cruz says he will not resign despite a “catastrophic” IT system failure that grounded scores of flights”

Paul Pester forced to stepping down as CEO of TSB after the disruption caused to millions of customers by the bank’s, very public, failed IT upgrade.

Former Equifax CEO Richard Smith says he is "deeply sorry" for the security breach in which sensitive personal information of as many as 143 million Americans was compromised.
Complex Technology Stack

Multi-language, multi-layer Architecture
- EJB
- PL/SQL
- Oracle
- SQL Server
- DB2
- T/SQL
- Hibernate
- Spring
- Struts .NET
- COBOL
- IMS
- Messaging
- Sybase

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
Everyone wants faster time to market, but few want to hear about the risks.
Complex Toolchains

• Design of the software and configuration
• Coding including code quality and performance
• Software build and build performance
• Release candidate

• Production metrics, objects and feedback
• Requirements
• Business metrics
• Update release metrics
• Release plan, timing and business case
• Security policy and requirement

• Infrastructure storage, database and network provisioning and configuring
• Application provision and configuration.

• Acceptance testing
• Regression testing
• Security and vulnerability analysis
• Performance
• Configuration testing

• Approval/preapprovals
• Package configuration
• Triggered releases
• Release staging and holding

• Performance of IT infrastructure
• End-user response and experience
• Production metrics and statistics
• Application monitoring
Increasing Technical Debt

- Code complexity
- Maintainability
- Internal Coupling
- Functional Size
- Redundant code
- Testability
- External Coupling
- Operating Cost
- Maintenance Cost
- Reliability
- Performance
- Business Value
- Maintenance Cost
MicroServices and API’s Can Accelerate Architecture Debt and Complexity

It's a nonlinear function that may level "S" or rise exponentially

It is not a linear function of the enterprise

One or Two Poor API’s Could Push You Over The Edge

In a nonlinear system, 90% of the complexity is a result of less than 10% of the node connections.
Example After 120 Day Project

Example After 120 Day Project

<table>
<thead>
<tr>
<th>Team Size</th>
<th>Inject Rate</th>
<th>Refactoring Rate</th>
<th>FTE Tech Debt Days Left</th>
<th>Refactoring Cost At $240</th>
<th>Refactoring Cost At $1040</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>5 - 15%</td>
<td>10%</td>
<td>16.3</td>
<td>$3,912</td>
<td>$16,952</td>
</tr>
<tr>
<td>10</td>
<td>5 - 15%</td>
<td>10%</td>
<td>32.7</td>
<td>$7,848</td>
<td>$34,008</td>
</tr>
<tr>
<td>20</td>
<td>5 - 15%</td>
<td>10%</td>
<td>65.3</td>
<td>$15,672</td>
<td>$67,912</td>
</tr>
</tbody>
</table>
## Example After 120 Day Project

### Average Team

<table>
<thead>
<tr>
<th>Team Size</th>
<th>Inject Rate</th>
<th>Rate</th>
<th>Days Left</th>
<th>At $240</th>
<th>At $1040</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>At $240</td>
<td>At $1040</td>
</tr>
<tr>
<td>5</td>
<td>10 - 25%</td>
<td>10%</td>
<td>63.2</td>
<td>$15,168</td>
<td>$65,728</td>
</tr>
<tr>
<td>10</td>
<td>10 - 25%</td>
<td>10%</td>
<td>126.4</td>
<td>$30,336</td>
<td>$131,456</td>
</tr>
<tr>
<td>20</td>
<td>10 - 25%</td>
<td>10%</td>
<td>252.8</td>
<td>$60,672</td>
<td>$262,912</td>
</tr>
</tbody>
</table>

### 3.8 X The Refactoring Cost Of A Good Team
Example After 120 Day Project

But wait…..what if its another team doing the refactoring and maintenance?

Then assume for each hour of coding by the original team allow between 2 to 8 hours by the maintenance team to understand and refactor the original code.
We Need Standards We Can Implement With DevOps

We built this city, we built this city on rock an' roll
We Need Standards We Can Implement With DevOps

We built this city, we built this city on rock an' roll
ISO 25010 Software Quality Model Is A Start

1. Functional Suitability
2. Performance Efficiency
3. Compatibility
4. Usability
5. Reliability
6. Security
7. Maintainability
8. Portability
ISO 25010 In Structural Code Analysis, Practical Examples

- **OWASP Top 10 Vulnerabilities**—most critical web application security risks – CWEs & CVEs

- **OWASP Application Security Verification Std v4.0** – 14 categories guide automated unit & integration tests – most all verification checks have corresponding CWEs

- **SANS/CWE Top 25** — most commonly encountered cyber weakness enumerators (CWEs),

- **CISQ Object Management Group (OMG)** Automated Source Code Measures for technical debt & structural quality (Security, Reliability, Performance Efficiency & Maintainability) – all based on MITRE CWEs
As industry's mature they automate, from robots to fly-by-wire
Building A Foundation Quality Standards That Fit Modern Methods and Architecture

Quality Standards That Are:

• Automated

• Product focused vs project

• Support Event and API Architecture

• Integrated in to DevOps & DevSecOps Toolchain
CISQ Structural Quality Measures

CISQ Structural Quality Measures

<table>
<thead>
<tr>
<th>Category</th>
<th>Number of Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>22 weaknesses (Top 25 CWEs)</td>
</tr>
<tr>
<td>Reliability</td>
<td>29 weaknesses</td>
</tr>
<tr>
<td>Performance Efficiency</td>
<td>15 weaknesses</td>
</tr>
<tr>
<td>Maintainability</td>
<td>20 weaknesses</td>
</tr>
</tbody>
</table>

Example architectural and coding weaknesses included in 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

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 of ownership.

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.
Certify The Environment Regards QA, Don’t Assume It
Not All Suppliers Teams Are Equal, Don’t Work With Poor Teams

Freeze Periods
- Only exceptional change freeze periods apply

Change Advisory Board
- CAB for information purposes only

Frequency of Deployments
- No limits on changes per today

Time of Deployments
- Intra-day allowed

Level of Automation
- Continuous Integration
- Quality Assurance
- Coding Practices
- Release Management
- Incident Management
- Environments
Link Automation to KPI, and Set Targets For Tech Debt Reduction

- Feature throughput
- Lead-time/Cycle-time
- IT Downtime
- Business Downtime
- Percentage of task automated
- Refactoring rate and cost
And Have a Quality Dashboard The Team Can Use To Control Debt
Focus on Outcomes

- Higher Productivity
- Business Outcomes
- Grater Agility
- Improves Quality
- Reduces Risk
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.”
Working With Suppliers

Six Levels of Engaging Vendors with CISQ Standards

**Recommendation email**
- Email to vendor delivery leaders that they should consider using CISQ guidelines for all ADM work

**RFP**
- Initial statement of requirements and project definition can set the tone for quality of deliverables

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

**SOW**
- Definition of specific project scope and deliverable can include definition of quality and security

**Scorecard**
- Measurement and discussion in governance committees to help set behavior

**Acceptance criteria**
- Measure and demand minimal set of acceptance criteria for any new development or release
CISQ/OMG Standards Process – Short Cycle

CISQ Executive Forums

OMG

OMG Approved Standards

ISO Fasttrack

Deployment Workshops

Automated Function Points

Reliability

Performance Efficiency

Security

Maintainability
## CISQ Get The Standards – They Are Free

### SOFTWARE SIZING

- **Automated Function Points**: Measures the functional size of software.
- **Automated Enhancement Points**: Measures changes in the size of both functional and non-functional code during a release in one measure.

### CODE QUALITY

- **Security**: Measures weaknesses in source code representing the most exploited security weaknesses in software including the CWE/Sans Institute Top 25 Most Dangerous Security Errors and OWASP Top 10.
- **Reliability**: Measures weaknesses in source code impacting the availability, fault tolerance, and recoverability of software.
- **Performance Efficiency**: Measures weaknesses in source code impacting response time and utilization of processor, memory, and other resources.
- **Maintainability**: Measures weaknesses in source code impacting the comprehensibility, changeability, testability, and scalability of software.

### TECHNICAL DEBT

- **Technical Debt**: A measure of corrective maintenance effort due to the CISQ code quality weaknesses remaining in a software application.

[https://www.it-cisq.org/standards/](https://www.it-cisq.org/standards/)
CISQ Work With Us

JOIN THE INDUSTRY-LEADING CONSORTIUM ADVANCING SOFTWARE QUALITY MEASUREMENT

The Consortium for Information & Software Quality™ (CISQ™) puts Information Technology (IT) leaders in the position to directly participate in the development of industry standards and methodologies for measuring the quality and trustworthiness of software. Members include IT executives and practitioners in charge of significant mission-critical applications from many enterprises, systems integrators and public sector institutions across the globe.

INDIVIDUAL MEMBERSHIP

Would you like to stay updated on this work and network with members in the community? Individual membership is free.

- Subscribe to CISQ’s email list
- Receive updates on the standards
- Receive technical guidance documents
- Receive event invitations

JOIN NOW

CORPORATE MEMBERSHIP

Would you like to contribute to the standards and participate in deployment activities? Your organization is invited to become a corporate member and sponsor the work that CISQ undertakes. Sponsorship is open to companies, government agencies, not-for-profit, and academic institutions.

- Team members participate in working groups
- An executive joins the Governing Board
- Your organization is listed as a supporter of all CISQ events, including complimentary passes and an exhibit table
- See benefits of corporate membership

JOIN NOW  I'M INTERESTED IN SPONSORSHIP