Quality in the Digital Age: CISQ and the Role of the SI in the Software Supply Chain

David Norton, Executive Director

October 30, 2019
"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.
Quality Starts With The System Integrator, They Build The Foundation Digital Business Is Based On

- Service & Products
  - API’s
  - App’s
  - IoT
  - Big Data
  - AI
- Business Unit
  - Business Unit
  - Business Unit
- Demand Management
  - Internal IT
  - Vendor Management
  - Compliance
- External Suppliers
  - SaaS Vendors
  - System Integrators
  - Package Providers

©2019 CISQ
Weaknesses and Vulnerabilities That Find Their Way Into Products & Services Have Devastating Effects

Service & Products

- Business Unit
- Business Unit
- Business Unit

Demand Management

- Internal IT
- Vendor Management
- Compliance

External Suppliers

- SaaS Vendors
- System Integrators
- Package Providers

API's
- App's
- IoT
- Big Data
- AI

©2019 CISQ
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

©2019 CISQ
The Blame Roles Down Hill

- Cyber Incident
- Outage
- Bad Press
- Chief Information Office
- Chief Security Office
- Head of Vendor Management
Banks blame 3rd party software for outage

SI let us down, sorry

It was not us, it was them
SI and Outsourcing Generally Is Feeling The Pressure – Not Just Because Of Quality & Cyber

- Over 60% of contracts renegotiated
- Over a 1/3 cancelled outright
- In-sourcing is on the rise
- SI losing out to SaaS
But Wait……

IT DOES NOT HAVE TO BE THIS WAY
Quality and Resilience This Way
SIs Should Be Proactively Using & Developing New Quality Practices and Standards To Support Digital
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 into DevOps & DevSecOps toolchain
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.
Benefits To The SI In Using Current CISQ Quality Standards

• Lower the amount of rework and by doing so improve customer relationships
• Lower indemnity risk and cost to the end customer
• Increase velocity and shorten lead-time without sacrificing quality or increasing risk
• Reduce technical debt for individual applications and portfolios leading to greater productivity
• Increase the size of the portfolio that can be developed and maintained without increasing headcount - more revenue and bigger margin
Building A Trust Relationship Based On Standards

RFP
Embed Software Quality & Sizing Standards Into Request For Proposal or Quotes
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 Information Software Quality (CISQ) for guidance on how to measure, evaluate and improve software.”
Embed The Agreed Sizing Method and Productivity Into The Statements of Work
Embed The Agreed Sizing Method and Productivity Into The Statements of Work

1. **Contracting and Productivity**

1. **Productivity**

   The contracted is based on a bases level of productivity of **18 Function Pointers per Staff Month** [1]. A staff month is defined as 22 days per calendar month, 8 hours per day, equalling 176 working hours per month.

   Attentively the contracted is based on a bases level of productivity of 9.5 hours per function point [1].

1. **Rate**

   The supplier shall invoice at a rate of €300 [2] per function point delivered to the client as measured by **ISO 19515 Information technology — Object Management Group Automated Function Points (AFP), 1.0** defined in section 3.4

   Exceptions to the rate and activities that will not be invoiced by function point must be agreed in advance of contract signing.
Suppliers Should Be Ready To Developer To The Standards
Suppliers Should Be Ready To Developer To The Standards
Suppliers Teams Should Use Tools That Support CISQ AFP/ISO Sizing Standards

Automatic Analysis Of The Size Of The Code In Function Points
Team Dashboards Should Clearly Show The Size Of Code Developed and Enhanced
Teams Are Still Free To Use Agile & DevOps Story Point Sizing, Automated Function Points Counted In The Background

Team A

Velocity = 25 SP

Product Backlog → Sprint Backlog → Sprint

2 Wks. → 24 h

Working increment of the software

Build → Integrate → Test → Deploy

Velocity (Relative)

Automated Function Points (Absolute)

©2019 CISQ
Do Not Just Focus On Size of The Code, Verify The Quality – Automatically
Do Not Just Focus On Size of The Code, Verify The Quality – Automatically

©2019 CISQ
Suppliers Teams Should Verify Code Quality, and Check For Vulnerabilities Against CISQ Standards

- **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**: A measure of corrective maintenance effort due to the CISQ code quality weaknesses remaining in a software application
End to End Trust Relationship Based On Standards
And If It Goes Wrong, CISQ Standards Become Your Armor From Friendly Fire

SI

Excuse “It’s the SI’s poor code”

Excuse “SI quality is inconsistent”

Excuse “SI is not proactive”

Client
By Engaging With CISQ, You...

- Collaborate on vision for Digital Quality
- Direct input into the development of standards
- Benefits from CISQ related PR
- Demonstrate leadership with customers and prospects
- Influence policy makers and regulators
And The Benefits Of the CISQ and OMG Standards Process – Months Not Years
Next Generation Digital Quality Standards - Engage
Thank you

David Norton
Executive Director
david.norton@it-cisq.org

Founded 2010
3,000+ members
750+ companies
7 adopted standards
www.it-cisq.org