



FOUNDED BY:



## CISQ NEWSLETTER

January 2018



### *Announcing the Embedded Extensions Project*



CISQ is launching a working group to produce specifications for extending the **CISQ Quality Characteristic Measures** into embedded software. Depending on the extensiveness of the embedded additions, these specifications will be submitted to OMG® either as revisions to the four existing standards through a Revision Task Force (RTF) or new specifications through Requests for Comment (RFCs).

The project team consists of delegates with expertise in embedded software from each participating sponsor, in addition to experts from the Software Engineering Institute and the Common Weakness Enumeration project at MITRE Corp. The first meeting is February 13-14 at MITRE in McLean, VA. Our plan is to submit specifications in Q3/Q4 this year.

Please join me in welcoming **Northrop Grumman** and **Tech Mahindra** as new CISQ sponsors. CISQ will benefit greatly from their expertise and contribution to the program.

We are excited to announce our next **Cyber Resilience Summit** will be held on March 20th at the OMG Technical Meeting in Reston, Virginia. CISQ will also deliver presentations at the March 19 **Cybersecurity and Internet of Things (IoT)** and March 21 **Modernization Summit** events hosted by OMG.

I look forward to seeing you there.

Dr. Bill Curtis  
Executive Director  
CISQ

### **New Automated Technical Debt Standard**

***For the first time, Technical Debt measurement becomes common currency for developers and tech managers!***

The CISQ measure of **Technical Debt** is a new OMG® standard for measuring the future cost of defects remaining in system source code at release. The cost to fix structural quality problems constitutes the principal of the debt, while the inefficiencies they cause until fixed, such as greater maintenance effort or excessive computing resources, represent compounding interest on the debt. Presented live January 16, 2018

[Click here to download the presentation deck](#)



[Click here to watch the webinar on YouTube](#)

**Registration is Now Open!**

## Cyber Resilience Summit, March 20, Reston, VA

<http://it-cisq.org/cyber-resilience-summit-mar-2018/>

The **Cyber Resilience Summit** will discuss standards and best practices for risk-managed digital transformation and the practical application of systems engineering to support agile acquisition, cloud readiness, big data, technical debt control, and cyber risk management of complex mission, C2, weapon and citizen-facing systems.

Confirmed to speak are National Cybersecurity Leaders from the White House to discuss government IT policy.



**CYBER RESILIENCE SUMMIT**

**Strategies to Modernize & Secure Government IT**

MARCH 20, 2018 IN RESTON, VA U.S.A.

CO-PRODUCED BY:  

- Cyber risk standards
- Technical debt
- Cloud readiness
- Agile acquisition
- Government IT policy

**RSVP TODAY!**

### Preventing the next Equifax... All CVEs have Root Causes in CWEs

A couple of key takeaways from the breach –

1. Developers commonly use third-party components, both open source and commercial-off-the-shelf, in their code and products. It is critical for the development team to maintain an inventory of its third party components to manage the component's source, versions, and patches. SAFECODE has published an excellent guide on the subject. Read: [Managing Security Risks Inherent in the Use of Third-party Components](#). In the case of Equifax, action came too late.
2. Basic security prevention can help to protect against CVEs and future zero-day vulnerabilities. A subset of CVEs are issued with a mapping to relevant CWEs. The CWEs represent the vulnerability's root causes and source vectors for exploitation. The Equifax CVE, for example, was mapped to CWE-20 (improper input validation) and OWASP A4 (broken access control) in the OWASP Top 10 2017.

[Read more on CISQ's blog](#)

### Upcoming Events

**Outsourcing World Summit (OWS) 18**, February 18-21, Orlando, FL hosted by IAOP. Save \$300 with the code **OWS18CISQ!** Anyone who uses this code is eligible for a free room night (two night minimum) for a stay at the host hotel during the dates of the event.

**AFCEA DC Cybersecurity Technology Summit**, February 27, Arlington, VA.

**OMG® Technical Meeting**, March 19-23, Reston, VA. Don't miss the [Cyber Resilience Summit](#), [Cybersecurity & IoT](#), and [Modernization Summit](#).

**SEI Software and Cyber Solutions Symposium 2018: Agile and DevOps**, March 26-28, Arlington, VA.

**NASCIO Midyear Conference**, April 22-24, Baltimore, MD.

**STAREAST**, April 29-May 4, Orlando, FL. CISQ members save \$200 off the registration fee with the code **SECM**.

**HACKNYC**, May 8-10, New York, NY. CISQ presents "Putting an End to Technical Debt."

[View CISQ's Event Calendar](#)

**Thank You CISQ Sponsors**



Cognizant

CGI

NORTHROP GRUMMAN

Tech  
Mahindra

SYNOPSYS

#### About CISQ

The Consortium for IT Software Quality™ (CISQ™) is an IT industry leadership group comprised of IT executives from the Global 2000, system integrators, outsourced service providers, and software technology vendors committed to introduce computable metrics standards for measuring software quality and size. CISQ is a neutral, open forum in which customers and suppliers of IT application software can develop an industry-wide agenda of actions for improving IT application quality and reduce cost and risk. [www.it-cisq.org](http://www.it-cisq.org)

By accepting this email and not responding with an unsubscribe request, you have consented or "opted in" to receive additional correspondence and promotions from OMG® and its associated partners and sponsors. Should you wish to opt-out in the future please visit <http://www.omg.org/cgi-bin/unsubscribe.cgi>.