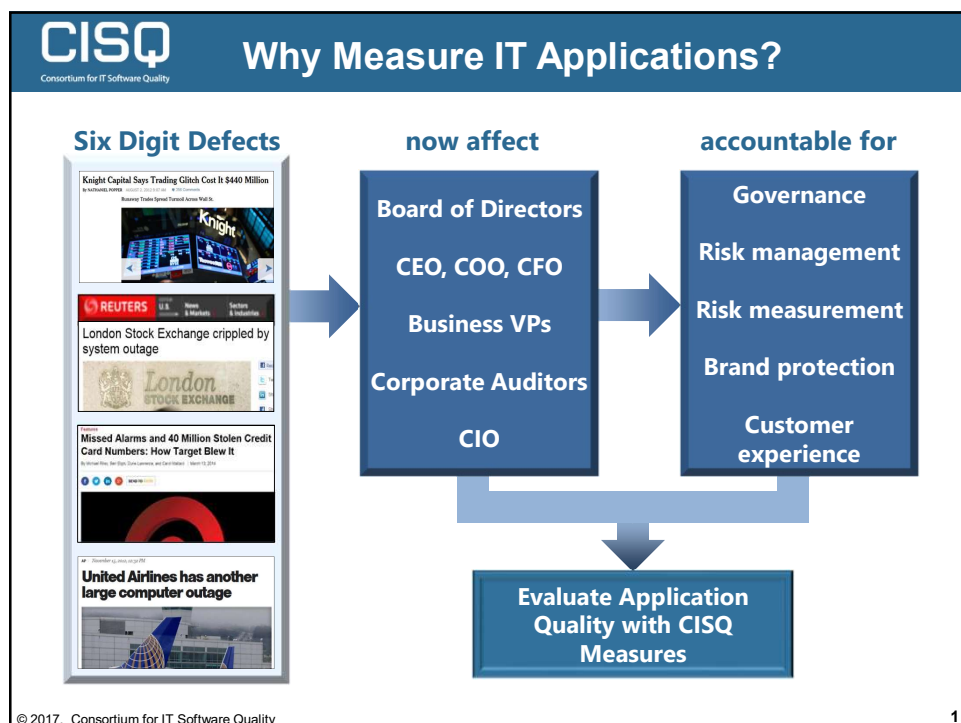


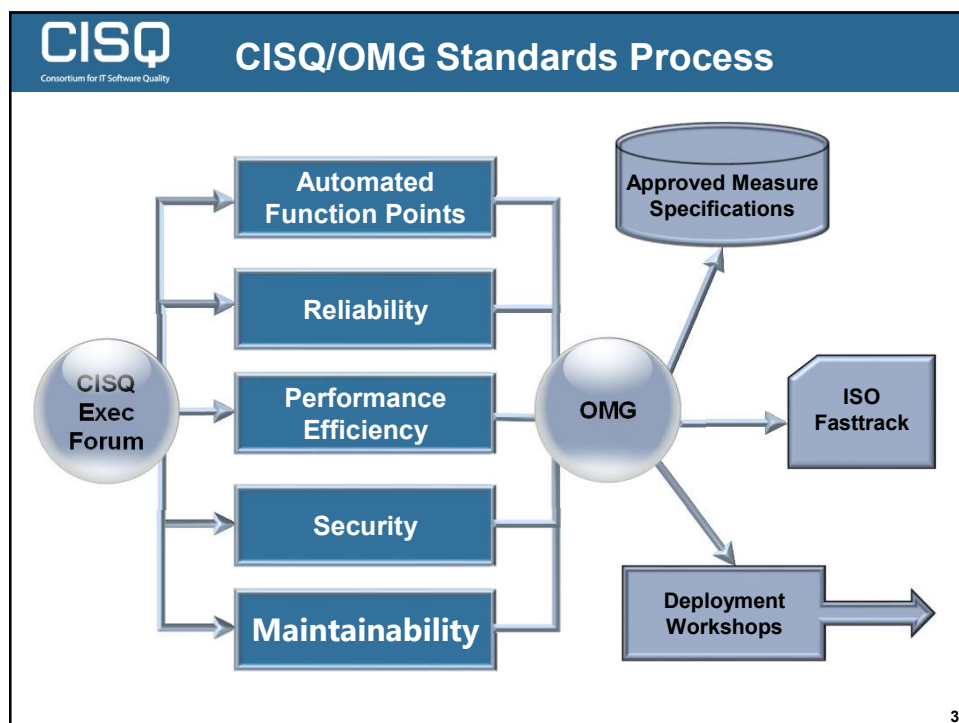
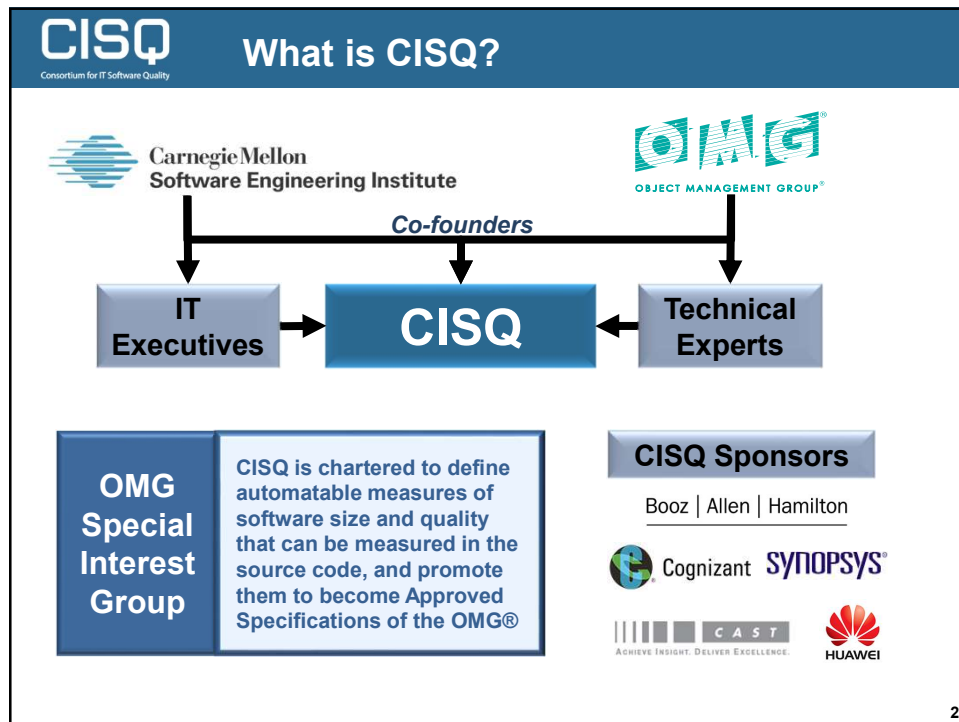
Software Security and Quality Issues in the Industrial Internet

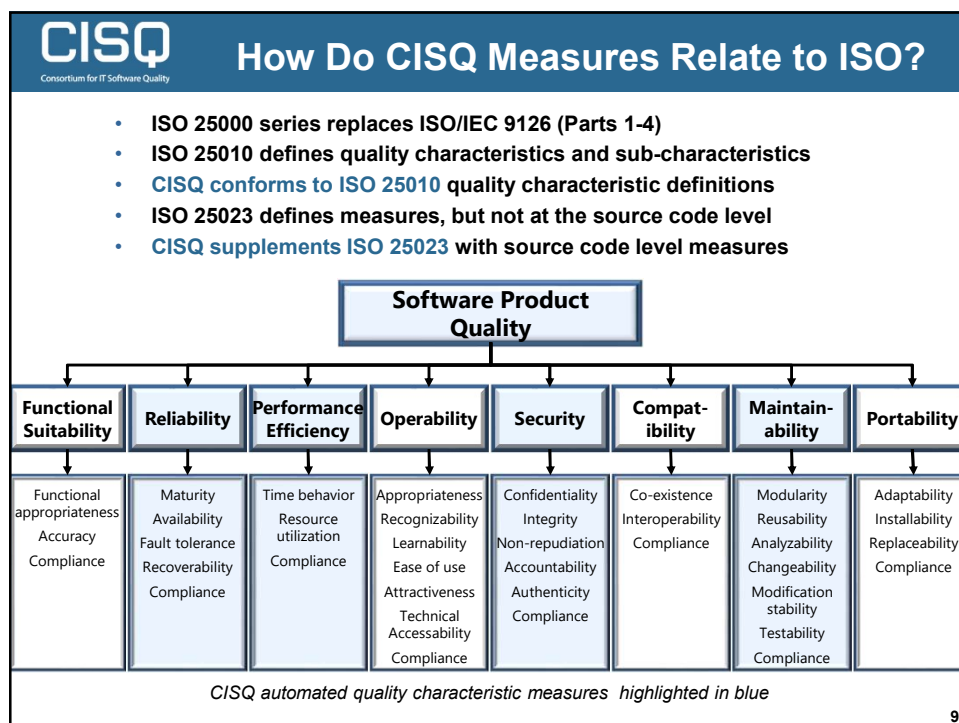
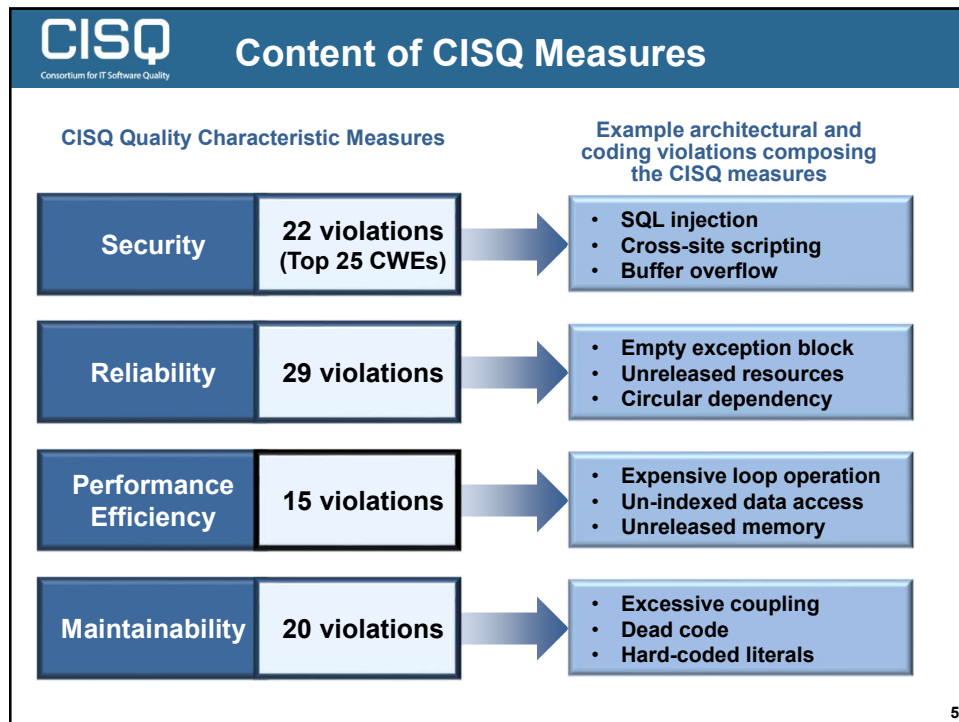
Dr. Bill Curtis
Executive Director


CISQ
Consortium for IT Software Quality













The 22 CWEs in the Security Measure

Consortium for IT Software Quality

- **CWE-22** Path Traversal Improper Input Neutralization
- **CWE-78** OS Command Injection Improper Input Neutralization
- **CWE-79** Cross-site Scripting Improper Input Neutralization
- **CWE-89** SQL Injection Improper Input Neutralization
- **CWE-120** Buffer Copy without Checking Size of Input
- **CWE-129** Array Index Improper Input Neutralization
- **CWE-134** Format String Improper Input Neutralization
- **CWE-252** Unchecked Return Parameter of Control Element Accessing Resource
- **CWE-327** Broken or Risky Cryptographic Algorithm Usage
- **CWE-396** Declaration of Catch for Generic Exception
- **CWE-397** Declaration of Throws for Generic Exception
- **CWE-434** File Upload Improper Input Neutralization
- **CWE-456** Storable and Member Data Element Missing Initialization
- **CWE-606** Unchecked Input for Loop Condition
- **CWE-667** Shared Resource Improper Locking
- **CWE-672** Expired or Released Resource Usage
- **CWE-681** Numeric Types Incorrect Conversion
- **CWE-706** Name or Reference Resolution Improper Input Neutralization
- **CWE-772** Missing Release of Resource after Effective Lifetime
- **CWE-789** Uncontrolled Memory Allocation
- **CWE-798** Hard-Coded Credentials Usage for Remote Authentication
- **CWE-835** Loop with Unreachable Exit Condition ('Infinite Loop')

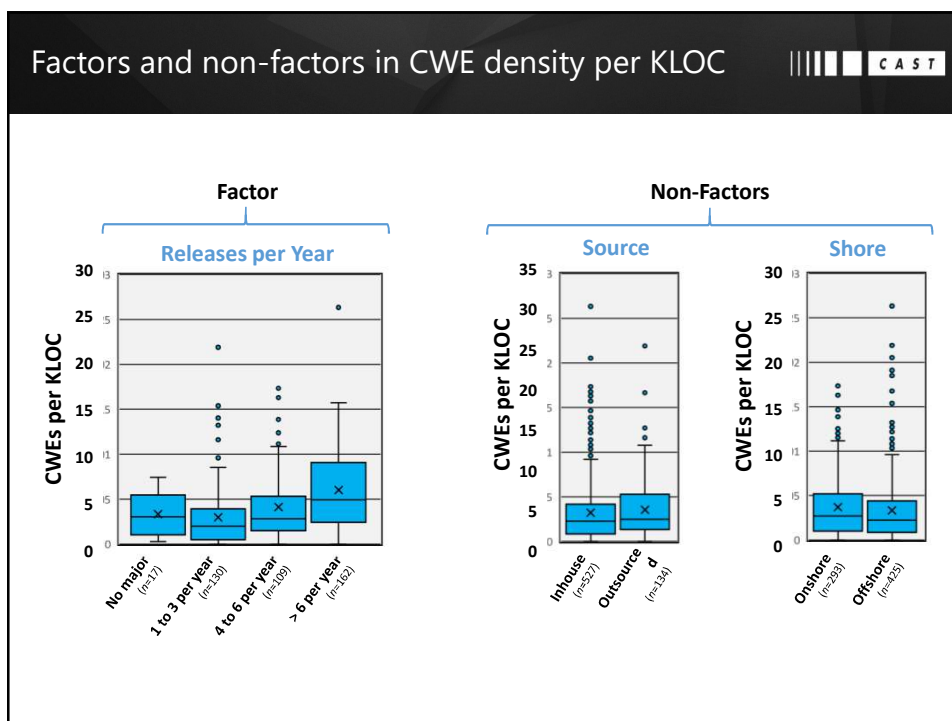


Robert Martin
MITRE



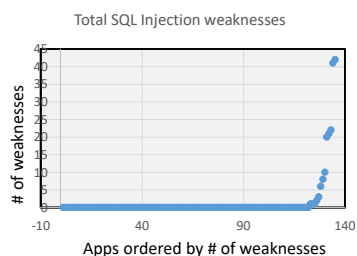
**Common
Weakness
Enumeration**
cwe.mitre.org

7

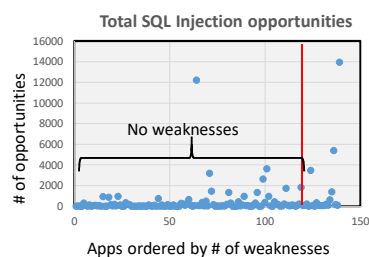


CWE-89 SQL injection

||| ||| CAST



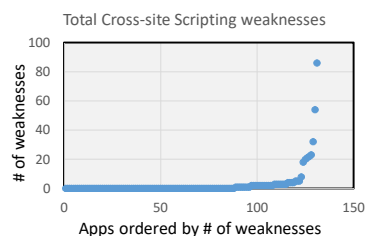
Statistic	Value	Range	Freq.	%
Mean	1.3	0	126	91
Median	0	1 to 2	4	3
Mode	0	3 to 9	4	3
Std. Deviat.	5.9	10 to 50	5	3
Range	4	>50	0	
Minimum	0			
Maximum	4			
Count	139			



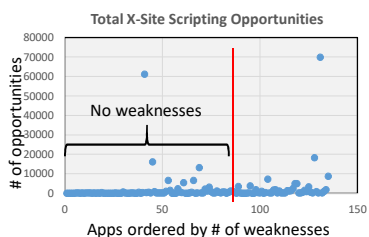
- SQL opportunities occurred in 9% of all apps
- SQL weaknesses occur in 9% of checked apps
- 3% of checked apps have extensive weaknesses
- Weaknesses unrelated to # of opportunities

CWE-79 Cross-site scripting

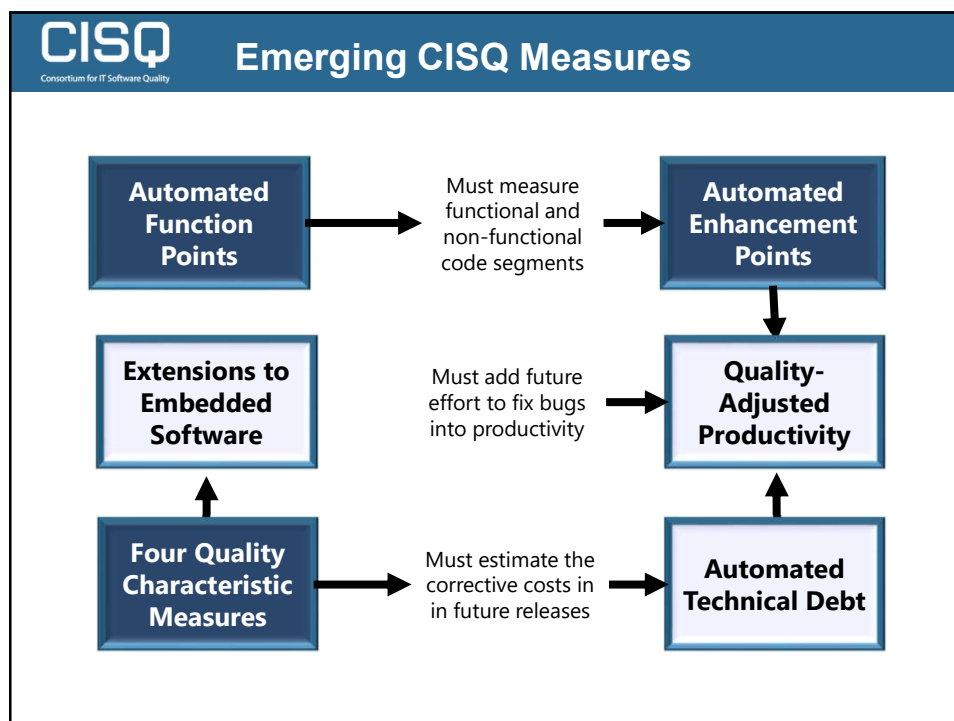
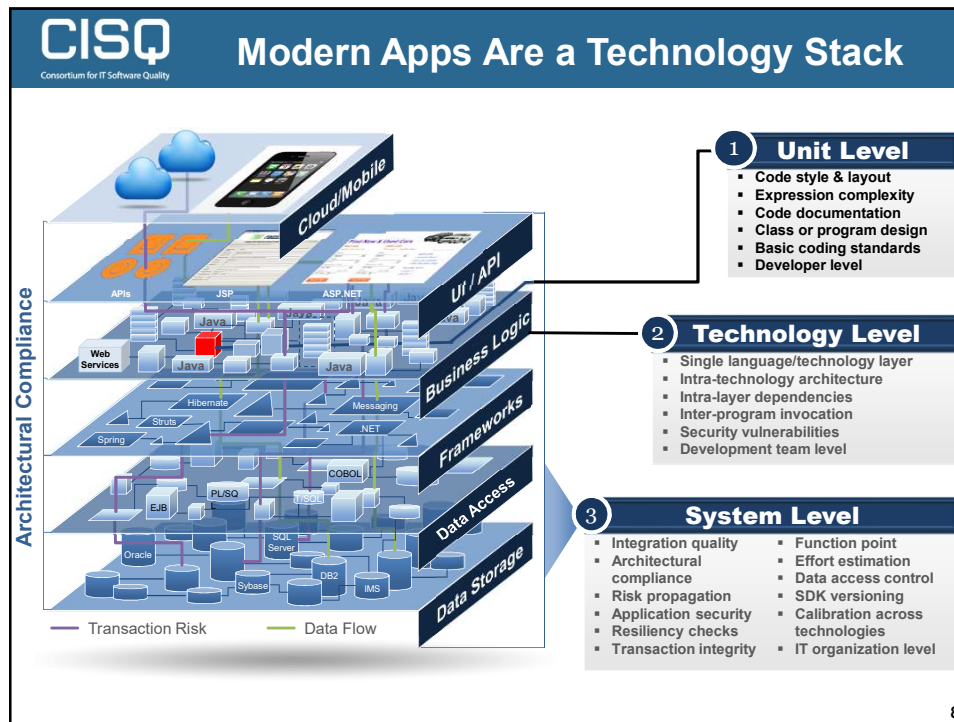
||| ||| CAST

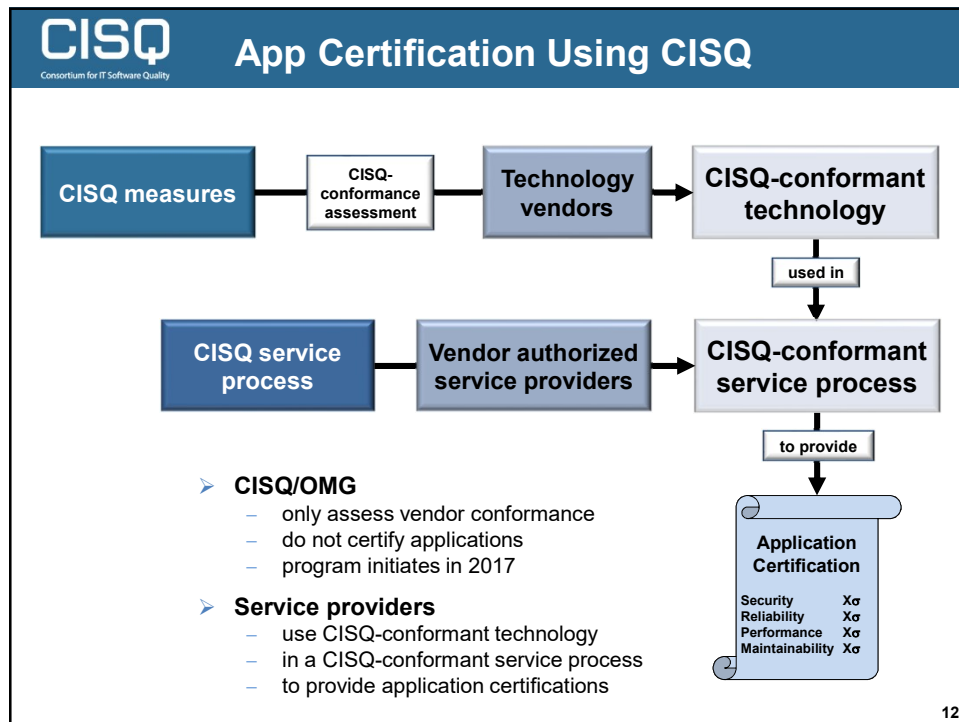


Statistic	Value	Range	Freq.	%
Mean	2.8	0	90	67
Median	0	1 to 2	20	15
Mode	0	3 to 9	17	13
Std. Deviat.	9.8	10 to 50	6	4
Range	86	>50	2	1
Minimum	0			
Maximum	86			
Count	135			



- X-site opportunities occurred in 9% of all apps
- X-site weaknesses occur in 1/3 of checked apps
- 5% of checked apps have extensive weaknesses
- Weaknesses unrelated to # of opportunities





CISQ
Consortium for IT Software Quality

Join CISQ ! www.it-cisq.org

CISQ
Consortium for IT Software Quality

FOUNDED BY: Software Engineering Institute Carnegie Mellon OMGA OBJECT MANAGEMENT GROUP

CISQ FAQs Contact Us

Search

Member Logout

Home Code Quality Standards Programs Members Area Blogs News and Events Wiki

Consortium for IT Software Quality

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 introducing a computable metrics standard for measuring software quality & 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 to reduce cost and risk.

Become a CISQ:

Member + CISQ Members Area

Sponsor + CISQ Events

CISQ Sponsors

SYNOPSYS Booz | Allen | Hamilton strategy and technology consultants CAST Cognizant HUAWEI

ADVANCING THE MEASUREMENT OF SOFTWARE SIZE, QUALITY, AND RISK

- ✓ Become a sponsor to lend thought leadership
- ✓ Join CISQ to stay current

CISQ

15