



# Managing Software Risk in a Multi-Sourced Environment

Marc Jones

Vice President Public Sector CAST Software &  
CISQ Director Public Sector (Volunteer)

Presentation Date: November 9<sup>th</sup>, 2017

# Why We're Here Today...

How effective would you say your current IT procurement process is, considering the following:

	Very Ineffective	Ineffective	Neither	Effective	Very Effective
Getting the most cost-savings for your state?	0	12%	20%	58%	10%
Getting the best value for your state?	0	8%	24%	53%	15%
Getting the most innovative technology for your state?	0	15%	31%	44%	10%

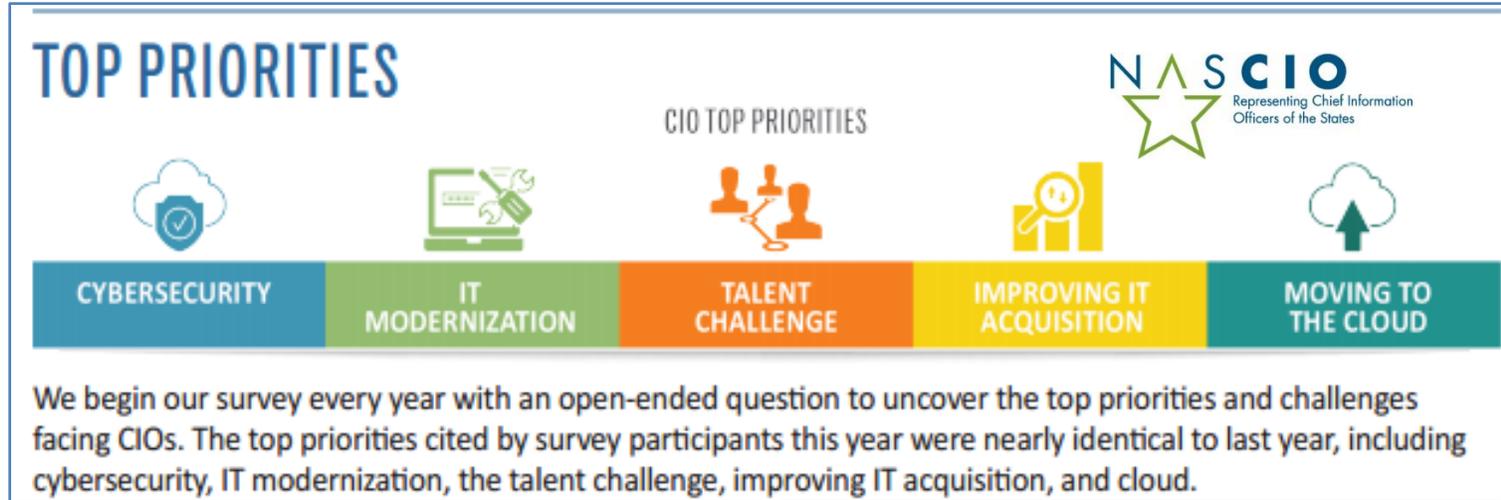
SOURCE- 2017 NASCIO/NASPO State IT Procurement Negotiations: *Working Together to Reform and Transform*

## Recommendation:

**Leverage enterprise architecture for improved IT procurement**

*The procurement process should be adjusted to recognize and align with enterprise IT strategies, architecture and standards based acquisitions.*

# How Software Standards Support Your Priorities (2016 Survey)



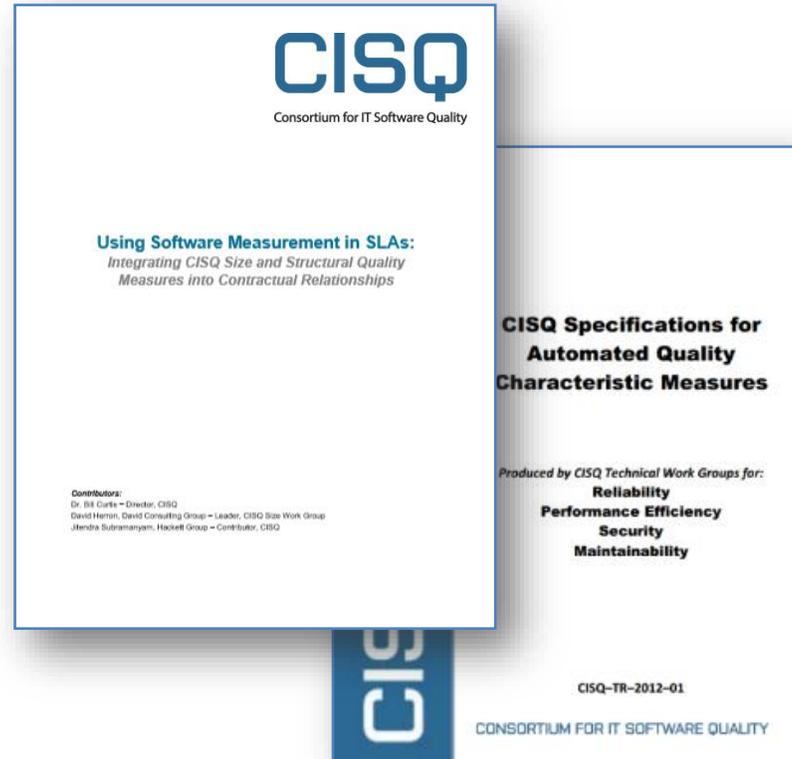
- **Cybersecurity** - Common criteria for *secure, resilient coding*, 50% app vulnerabilities are architecture\*
- **Modernization** – Benchmark/Remediate today’s risk, ensure tomorrow’s *sustainability* in dev & maintain
- **Talent Challenge** - Leverage standards and requirements to *promote current best practice*
- **IT Acquisition** - **Common** ‘non-functional’ *criteria*, often not in requirements – needs to be.
- **Cloud** - Assess/Benchmark current applications for scalability, portability (platform independence), security

\* Gary McGraw, *Software Security, Building Security In*

# CISQ: Acquisition Ready Standards-Based Measurements

## ▶ Consortium for IT Software Quality (CISQ)

- Goal is to improve IT application quality and reduce cost and risk
- Introduce a **computable metrics standard** for measuring **software quality & size**
- IT executives from Global 2000, system integrators, outsourced service providers, and software technology vendors
- NASCIO Member



## ▶ Object Management Group (OMG)



- Technology standards consortium
- Focuses on **enterprise integration standards** for a wide range of technologies and industries
- Modeling standards include Unified Modeling Language (UML) and Model Driven Architecture (MDA)



## MITRE

*MITRE is a private, not-for-profit corporation that operates FFRDCs—federally funded research and development centers. If you've ever flown in a jet or used GPS, you've benefited from technology with roots in an FFRDC.*



*We research software and cybersecurity problems of considerable complexity, create and test innovative technologies, and transition maturing solutions to widespread use.*

## Current CISQ.org Sponsors Include:



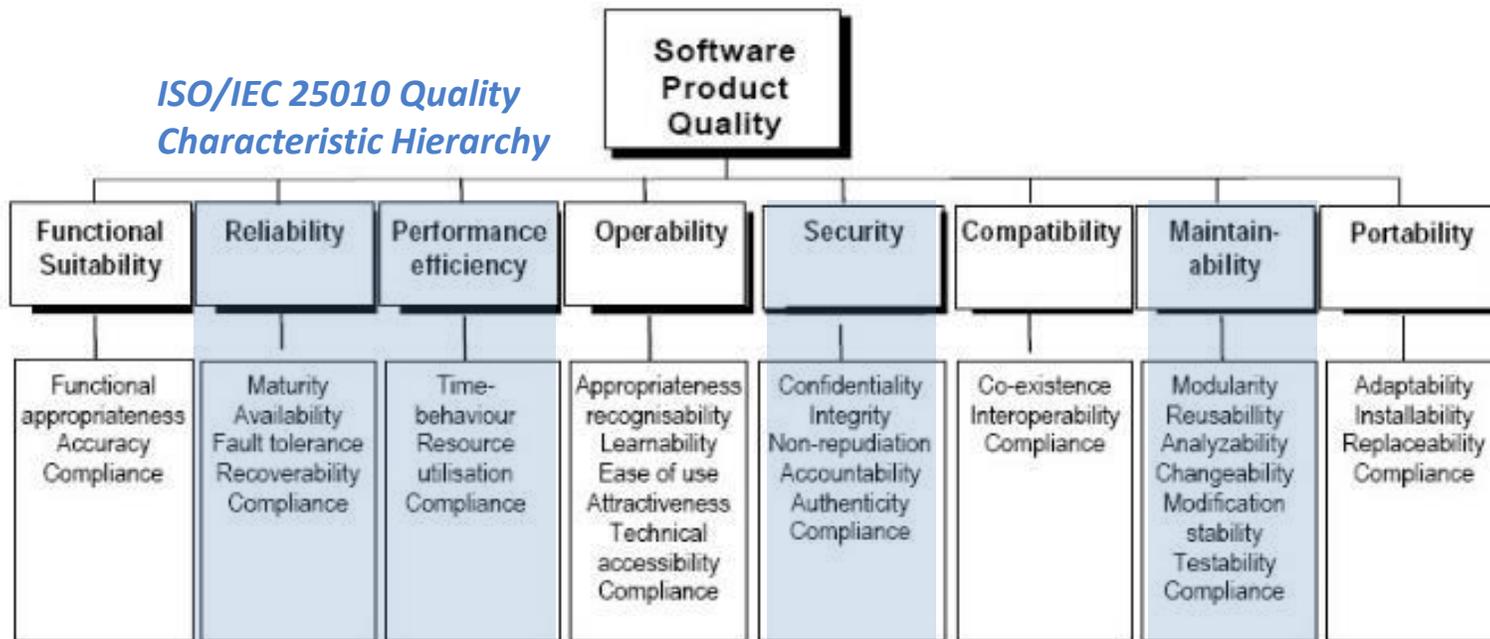
# CISQ Quality & Sizing Standard Approved for Public Sector Use

- Complies to international norms (ISO = International Standards Org.)
- CISQ conforms to ISO 25010 quality characteristic definitions
- CISQ supplements ISO 25023 with source code level measures
- Workgroups to focus on Portability & Compatibility (Cloud and IOT)

... and a surprise priority for the software work groups:

## AUTOMATED SIZING MEASURES:

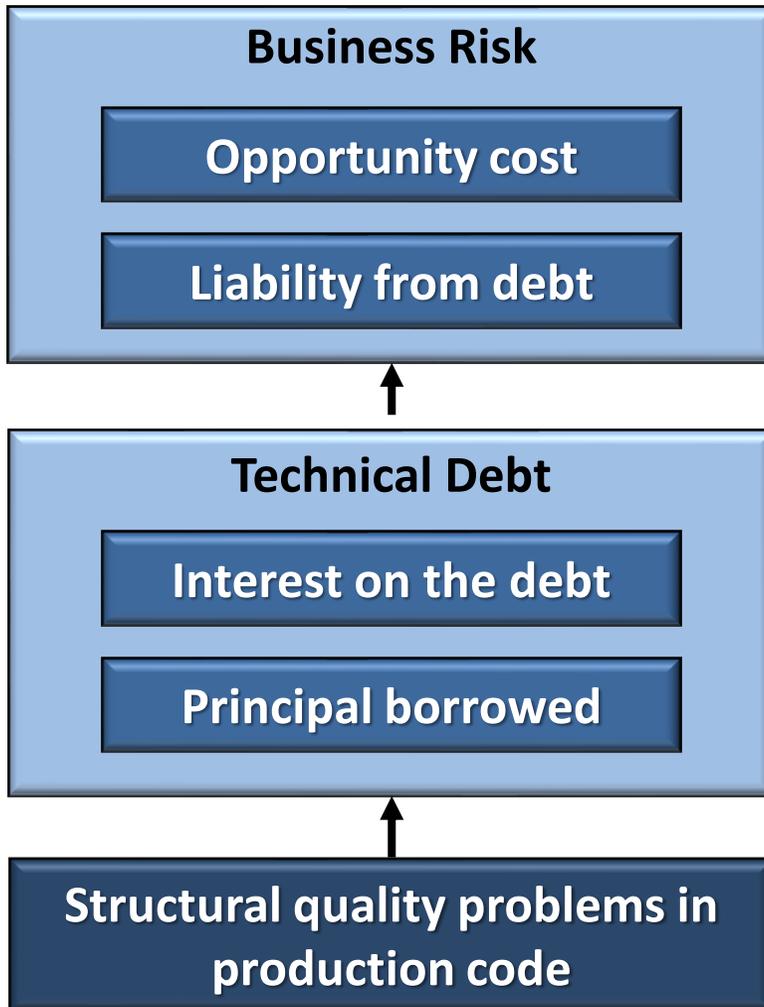
- Automated Function Points (AFP) for sizing applications. (Approved 2013)
- Automated Enhancement Points (AEP) for measuring effort and correlating throughput in development and sustainment effort. (Approved by OMG 2017)
- Coming Soon: **Technical Debt!**



CURRENT CISQ defined automatable measures for quality characteristics highlighted in blue. Approved 2015.

# What is Technical Debt? Why Should your State Care?

**Technical Debt** — the future cost of defects remaining in code at release, a component of the cost of ownership



**Opportunity cost**—benefits that could have been achieved had resources been put on new capability rather than retiring technical debt

**Liability**—business costs related to outages, breaches, corrupted data, etc.

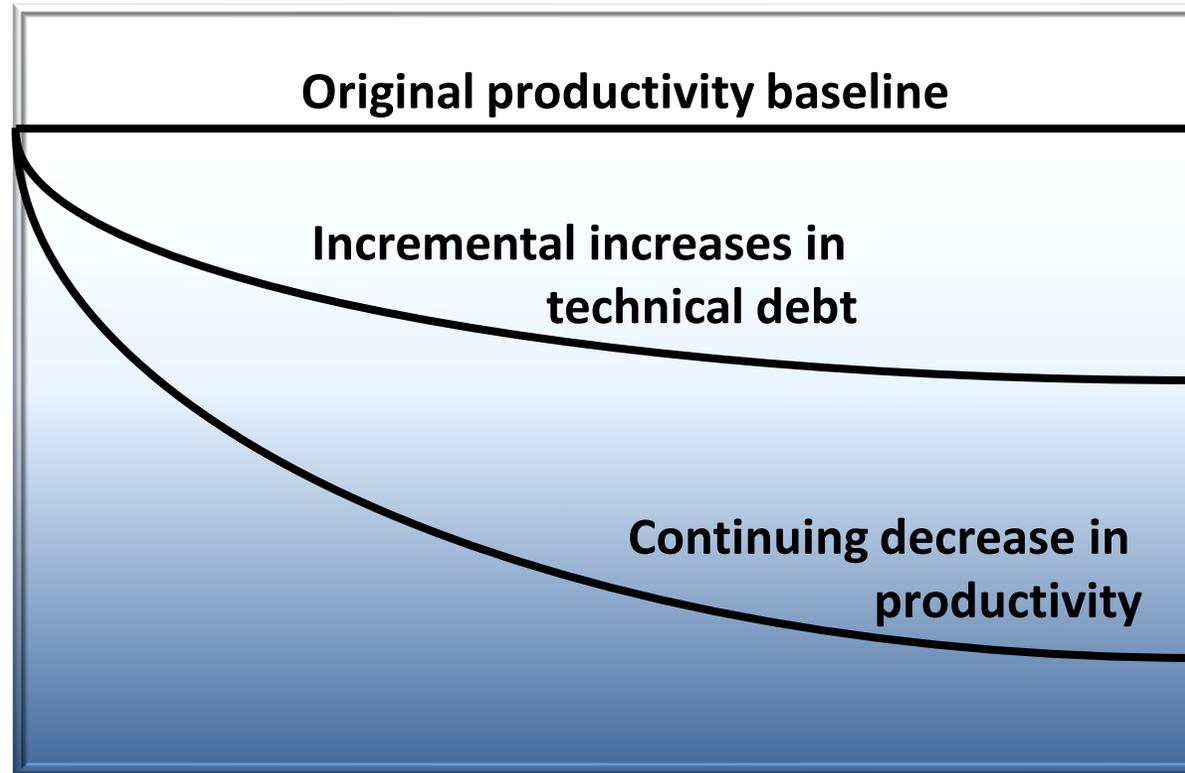
**Interest**— continuing IT costs attributable to the violations causing technical debt, i.e., *higher maintenance costs, greater resource usage, etc.*

**Principal**—cost of fixing problems remaining in the code after release that must be remediated

# How Accrual of Technical Debt Affects Productivity

**Assumption:** Productivity is a stable number

**Reality:** Productivity is a monotonically decreasing function of releases which increases enhancement and sustainment costs



What % of your states AD budget is sustainment?  
How do you reduce that over time?

# At Fed Level: Congress Mandates Software Quality Checks to DOD

## H.R. 3304

Directs the Secretary to provide for the establishment of a joint federation of capabilities to support the trusted defense system needs (security of software and hardware) of DOD. Requires the Secretary to determine whether the federation's purpose can be met by existing centers within DOD and, if not, to devise a strategy for creating and providing resources to fill such gaps.

### SEC. 937. JOINT FEDERATED CENTERS FOR TRUSTED DEFENSE SYSTEMS FOR

THE DEPARTMENT OF DEFENSE.

(a) Federation Required.--

(1) In general.--The Secretary of Defense shall provide for the establishment of a joint federation of capabilities to support the trusted defense system needs of the Department of Defense (in this section referred to as the "federation")

(2) Purpose.--The purpose of the federation shall be to serve as a joint center of excellence to support the trusted defense system needs of the Department to ensure security in the software and hardware developed, acquired, maintained, and used in support of the systems strategy of the Department and supporting policies related to software assurance and supply chain risk management.

**...the requirements for the discharge by the federation, in coordination with the Center for Assured Software of the National Security Agency, of a program of research and development to improve automated software code vulnerability analysis and testing tools**

## H.R. 4310

Directs the Under Secretary to: (1) develop and implement a baseline software assurance policy for the entire lifecycle of computer software acquired for DOD critical information, business, and weapons systems; (2) collect data on, and measure the effectiveness of, such policy; and (3) brief the defense and appropriations committees on additional means of improving software assurance and vulnerability detection.

### SEC. 933. IMPROVEMENTS IN ASSURANCE OF COMPUTER SOFTWARE PROCURED

BY THE DEPARTMENT OF DEFENSE.

(a) Baseline Software Assurance Policy.--The Under Secretary of Defense for Acquisition, Technology, and Logistics, in coordination with the Chief Information Officer of the Department of Defense, shall develop and implement a baseline software assurance policy for the entire lifecycle of covered systems. Such policy shall be included as part of the strategy for trusted defense systems of the Department of Defense.

(b) Policy Elements.--The baseline software assurance policy under subsection (a) shall--

(1) require use of approved and certified vulnerability analysis tools in computer software code during the entire lifecycle of a covered system, including during development, operational testing, **standards to achieve software security, assurance, and quality ...**

# Policy Examples Referencing Standards

- Requirements to assure software risk at the core portfolio level is becoming more common.
  - Internal Developed
  - Outsourced
  - Open Source
  - In the cloud
  - On Prem...

Documents redacted from slide for distribution

# Current Examples in July 2017 RFP's

Information Technology and Development Services  
GSA Schedule 70 BPA



General Services Administration  
Office of Chief Information Officer  
For the

Office of Public Buildings Information Technology Services

## Statement of Work & Request for Quotes

GSA Schedule 70  
Blanket Purchase Agreement (BPA)  
for

Information Technology and Development Services (ITDS)

### 5.9 Quality Requirements (Task Area 15)

The Enterprise Quality Program (EQP), provides the foundation for continuously improving, managing, and controlling the quality of software products for PB-ITS. Contractors shall follow PB-ITS Enterprise Quality Program (EQP) standards and practices. All deliverables shall be produced and delivered in accordance with PB-ITS's current EQP requirements provided in the Enterprise Quality Configuration Management Plan and the Release Matrix in Appendix A. The Government PM shall notify the Contractors, verbally or in writing, of deficiencies in the quality of deliverables and allow five (5) business days for a revision to be submitted.

PB-ITS 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) (<http://it-cisq.org/standards/>) for guidance on how to measure, evaluate and improve software. Particular areas of importance are Performance Efficiency, Reliability, Maintainability and Security. Contractors shall perform architectural and coding best practices within their development environments in order to deliver efficient, secure and reliable products to the Government. GSA currently uses a suite of tools and processes to assess the efficiency, security and reliability of code in applications.**

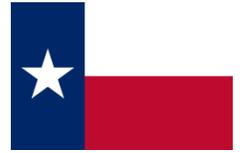
The Contractor shall adhere to CST application coding standards intended to assist in creating code that is free of critical quality defects and is highly maintainable. CST will employ a Software Code Review process by which it will analyze all source code by measuring application level code quality and code assurance across the portfolio of COTS configurations and custom developed software. **CST will also employ Software Code Quality (SCQ), an analysis that will evaluate application risk around robustness (stability, resiliency), performance, architectural security, transferability, system maintainability (sustainment) and changeability of applications as they evolve. These measurements are based upon industry best practices and standards related to complexity, programming practices, architecture, database access and documentation. They are derived from standards bodies such as the International Organization for Standardization (ISO), Software Engineering Institute (SEI), Object Management Group (OMG) and the National Institute of Standards and Technology among others.**

CST will leverage static code analysis tools, including **CAST Software's Application Analytics and Engineering Dashboards** with quality as its main focus to expose quality defects and ensure that code complies with established code quality metrics across all source language components that comprise the complete deployable software modules delivered under this base IDIQ and associated task orders issued thereunder.

Business capability.



# Now at State Level: Texas HB 3275 as of January 1, 2018



AN ACT relating to the monitoring of major information resources projects by the Department of Information Resources.

... Sec. 2054.1183. ANNUAL REPORT ON MAJOR INFORMATION RESOURCES PROJECTS. (a) Not later than December 1 of each year, the quality assurance team shall report on the status of major information resources projects to the:

(1) governor; (2) lieutenant governor; ...

(b) The annual report must include:

(1) the current status of each major information resources project; and

(2) information regarding the performance indicators developed under Section 2054.159 for each major information resources project at each stage of the project's life cycle.

SECTION 2. Subchapter G, Chapter 2054, Government Code, is amended by adding Section 2054.159 to read as follows:

Sec. 2054.159. MAJOR INFORMATION RESOURCES PROJECT MONITORING. (a) For the entire life cycle of each major information resources **project, the quality assurance team shall monitor and report on performance indicators for each project, including schedule, cost, scope, and quality.\***

(b) The department by rule shall develop the performance indicators the quality assurance team is required to monitor under Subsection (a). In adopting rules under this subsection, the department shall consider **applicable information technology industry standards.**

(c) If the quality assurance team determines that a major information resources project is not likely to achieve the performance objectives for the project, the quality assurance team shall place the project on **a list for more intense monitoring** by the quality assurance team.

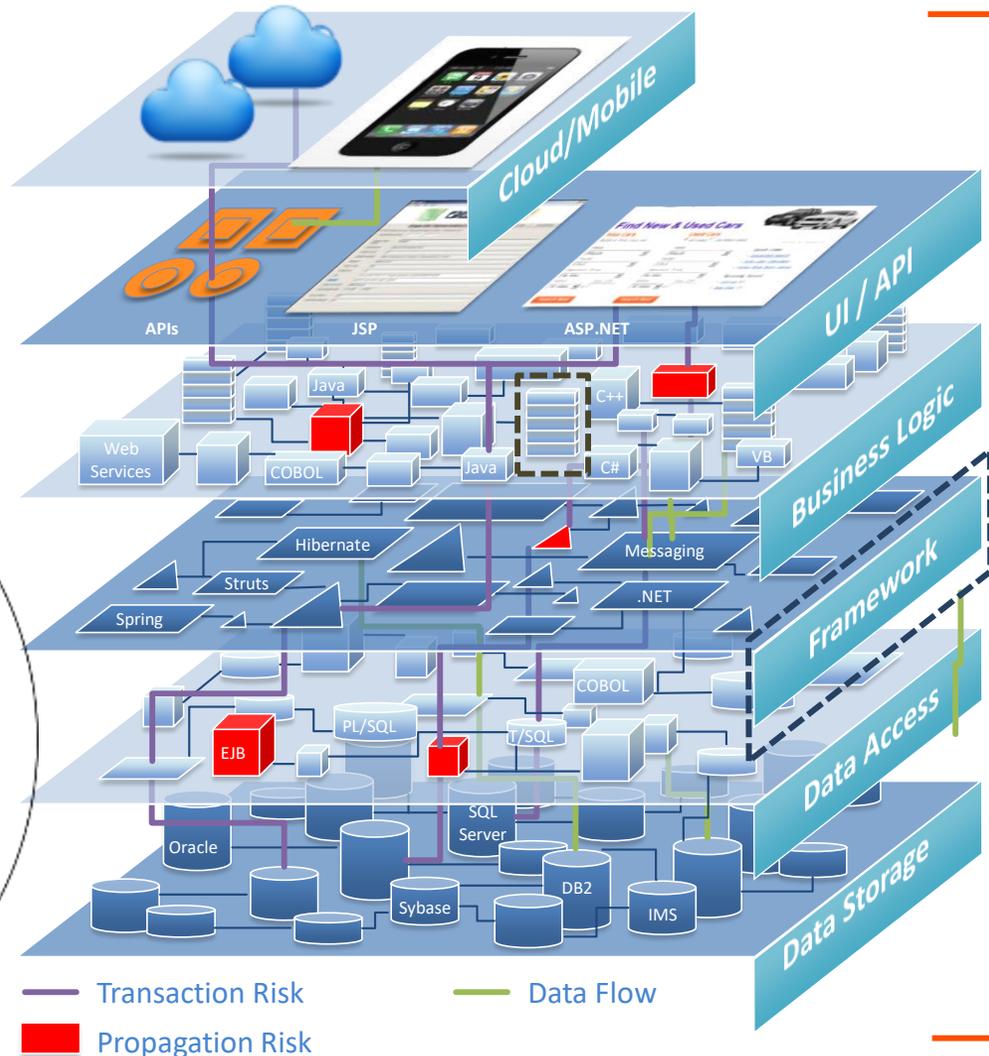
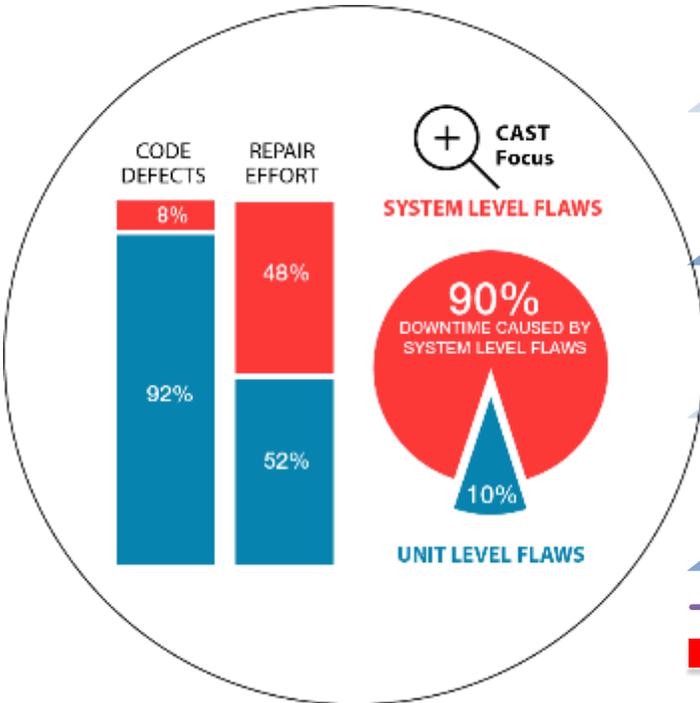
(d) The quality assurance team shall closely monitor monthly reports for each major information resources project identified under Subsection (c) and, based on criteria developed by the department, determine whether to recommend to the executive director the need to initiate corrective action for the project.

(e) The department shall create and maintain on the department's Internet website a user-friendly data visualization tool that provides an analysis and visual representation of the performance indicators developed under Subsection (b) for each major information resources project. ...

\* CISQ

# CISQ: Complex Programs Require – Architecture-Level Measurement

“Studies show that system-level coding problems, as opposed to code quality within a component, lead to 90% of production outages.”



## Code / Unit Level Quality Tools

- Typically open source or JIDE/Developer level Code style & layout focus



## Technology Level Quality Tools

- Single language / technology layer
- Intra-technology architecture



## System Level / Structural Risk

- Integration quality
- Architectural compliance
- Transaction Integrity & Security
- Calibration across 50 technologies
- Benchmark over time, across portfolio and with Industry data.



“...most devastating defects can only be detected at the System Level.”

Object Management Group Research (R. Soley)



# Improve Collaboration in Multi-sourced Environment

PROGRAM  
CENTER OF  
EXCELLENCE



- Provide scorecards to current software vendors
- Provide guidelines to vendors wanting to do business
- Use metrics as procurement SLAs for requirements, awarding, and administering
- These firms have CAST capability in house:

Infosys

IBM

Capgemini  
CONSULTING. TECHNOLOGY. OUTSOURCING

Cognizant

Booz | Allen | Hamilton

CGI

WIPRO  
WORLDWIDE LEADERSHIP

accenture  
High performance. Delivered.

NASCIO

## Roles & Responsibilities

### OIT and Agency CIOs



- Understand Software Standards
- Advocate awareness and acceptance

### Program Management/Engineering Leads / Program Owner



- ID at risk programs
- Ensure adherence to standards

### Contractor or Gov Dev & Assessment Engineers



- Upload source code
- Commitment to improvement

## Deliverable



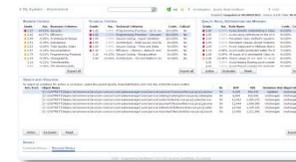
Reg Summary Report



Application Report



Application Analytics Dashboard



Engineering Dashboard

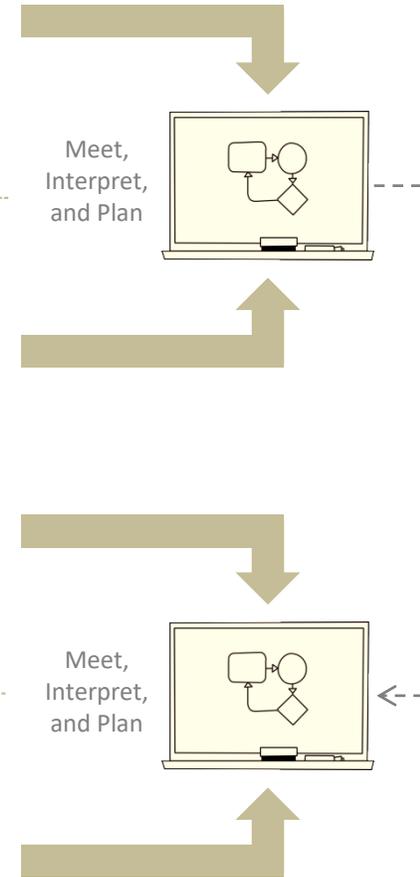
## Action Items

- At-Risk Applications (New Critical Violations, Increase in Risk indicators., etc.)
- Evaluate Risk Reduction Progress across programs (Leaders, Laggards, Best Value Hot Spots)

- Application Hotspots
- Remediation Trends
- Recommended Remediation Priorities

- Quality and critical violations trend
- Common / repeating violations

- Deep dive investigation into violations
- Learn best practices
- Formulate remediation plan



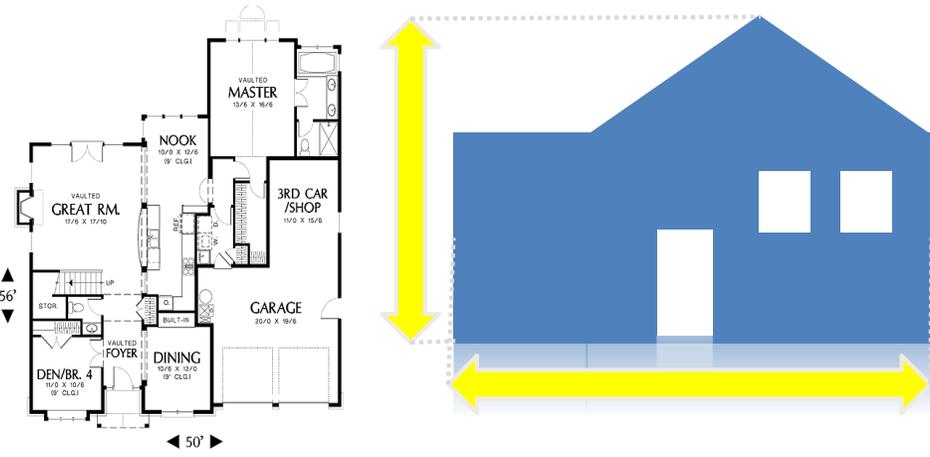
# Sizing Systems: Challenge in Agile Acquisition & Program Governance

Story points are the most commonly agile sizing criteria. However they are not effective for evaluating throughput. Function points have historically proven to be the most accurate throughput method, but are hard to incorporate into automated agile/devops environments as they are manually count. CISQ's automated functional sizing resolves this issue.

Forrester graphic not approved for distribution

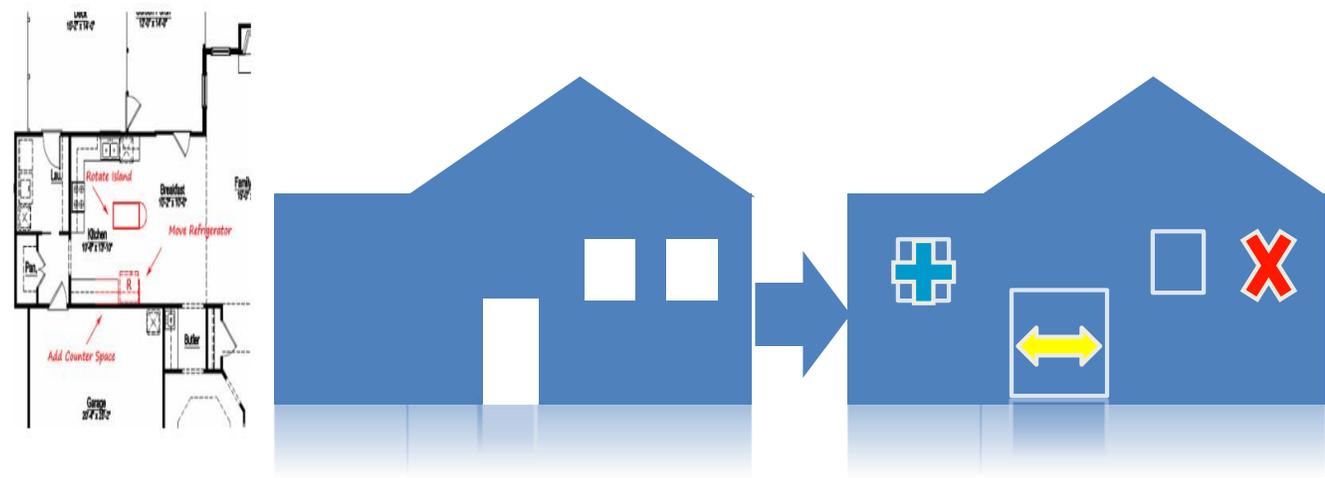
# How “Big” is your Software? Why is that Important to Know?

## Automated Function Points



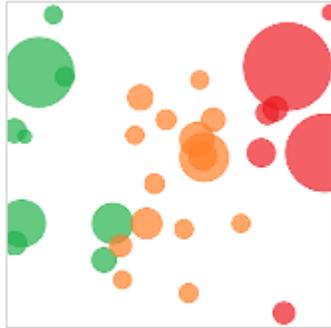
- Measure the **total** amount of business or mission functionality in a system.

## Automated Enhancement Points



- Measure Development & Sustainment & Rework
- Only measure # of modifications between two versions.
- added + updated +deleted)
- True measure of effort.

# CAST Analytics: Trailblazing to Put CISQ Measures into Action



Portfolio-level risk and saving opportunities



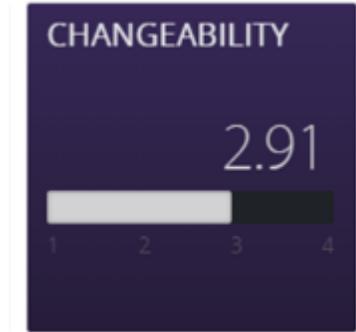
Likelihood of outage, data integrity or reliability issues



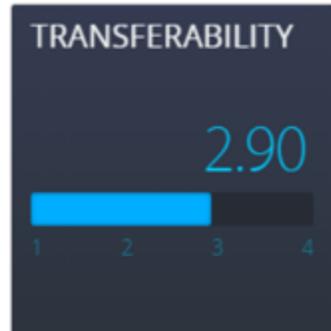
Resource consumption, scalability and performance issues



Security issues and high likelihood of breaches



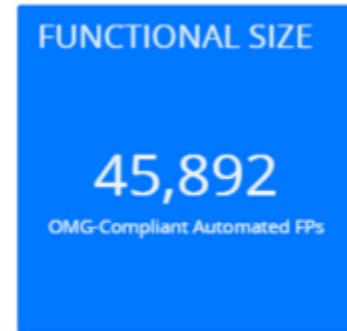
Adaptability to changing regulations and business needs



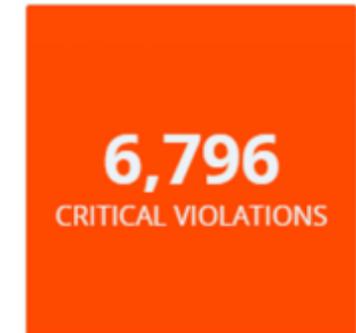
Ramp up difficulties for newcomers



Standardized units of ADM work with consistent technical and functional sizing for productivity measurement

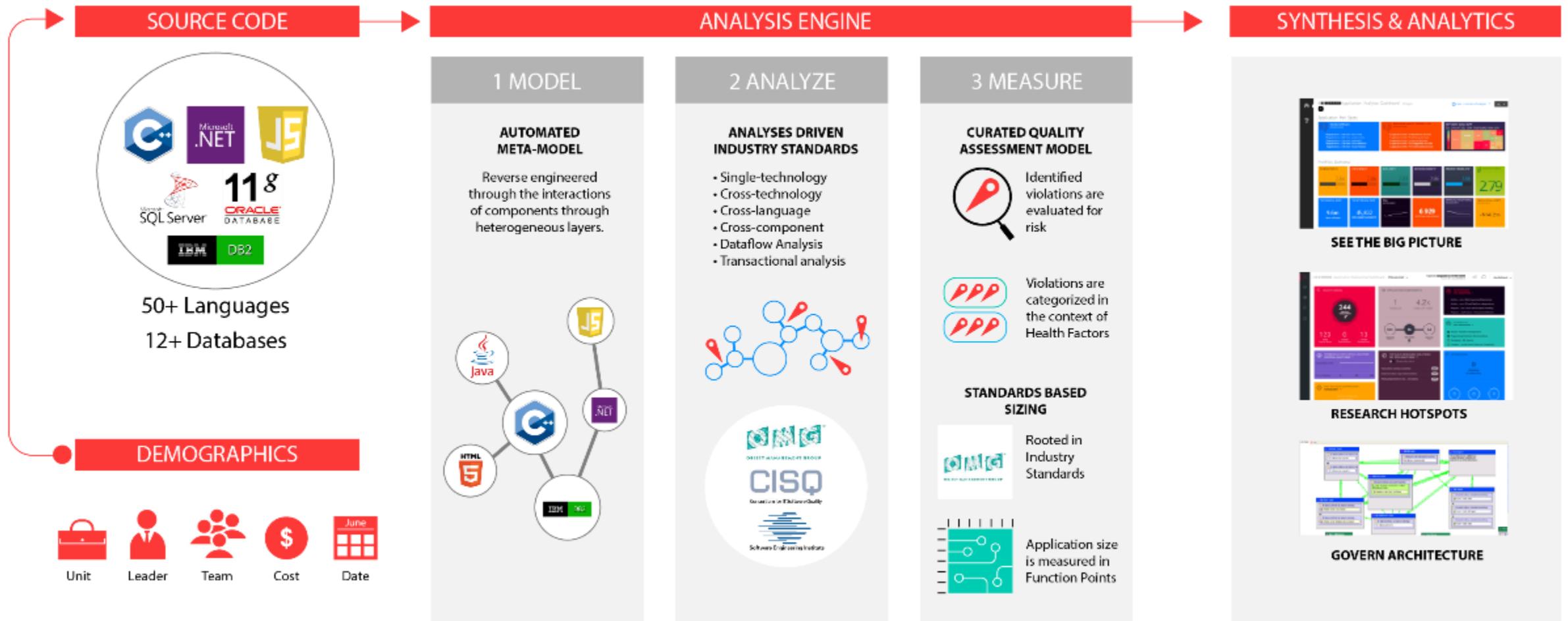


Cost to restore applications back to healthy state



Hard-to-find structural flaws that may lead to software catastrophes

# CAST AIP: System Level Analytics for the Enterprise



# Client Example: Scorecard Using Function Point Data + Quality

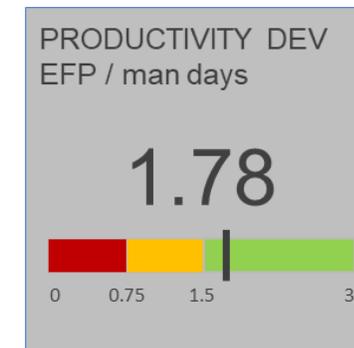
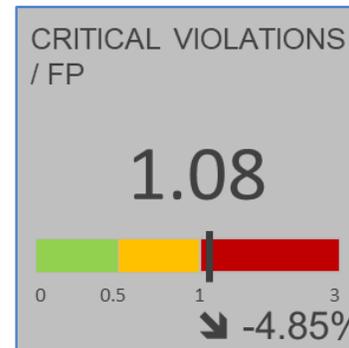
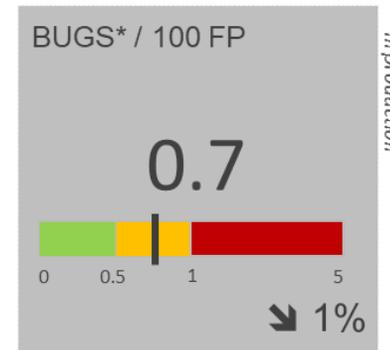
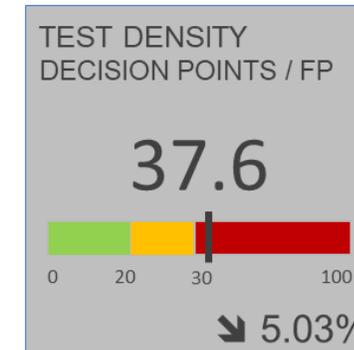
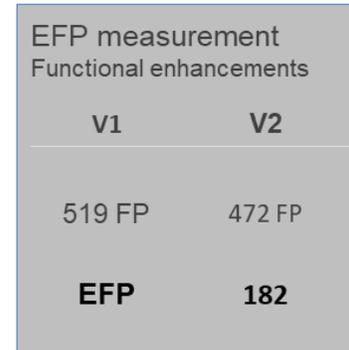
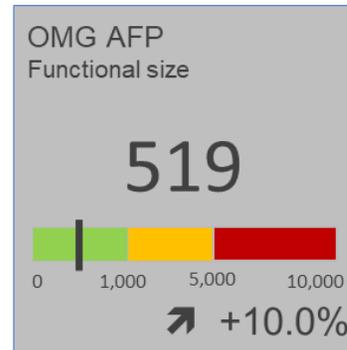
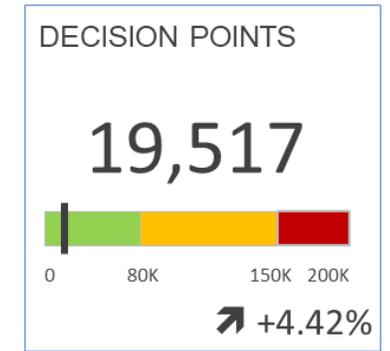
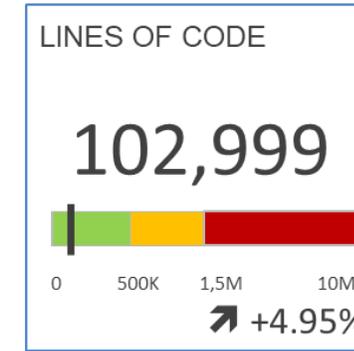
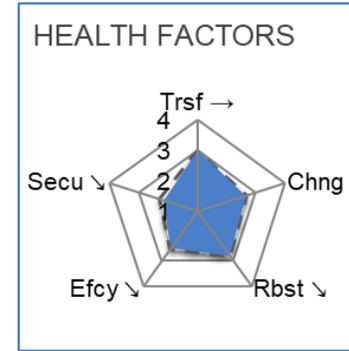
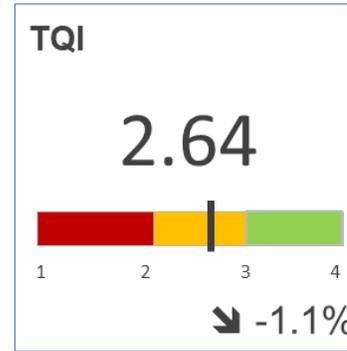
**Client objective is to track Unit Cost data at a departmental level**

This is an internal scorecard for IT management to track how well IT is doing, and to set internal KPIs

Combination of FPs, LOCs and decision points provides a triangulation of size & complexity data

Scorecard is a combination of CAST and external data

***Risk Adjusted Productivity***



\* In production

# Bringing It All Together at Agile Speed

Client's Output Screen redacted from slide for distribution

# A Recent 2017 Event...



8:30	<b>Welcome Remarks</b> <ul style="list-style-type: none"><li>– Dr. Bill Curtis, Executive Director, Consortium for IT Software Quality (CISQ)</li><li>– John Weiler, Vice Chair, IT Acquisition Advisory Council (IT-AAC)</li></ul>
8:45	<b>Opening Keynote Panel</b> <ul style="list-style-type: none"><li>– Tony Scott, former Federal Chief Information Officer</li><li>– Greg Smithberger, CIO/CTO, NSA</li></ul>
9:15	<b>Titans of Cyber Panel: Policy and Directives for Modernizing and Securing Legacy IT</b> <b>Topics: FITARA, MGT Act, Executive Order for Cyber Security</b> <b>Lead: Dr. Edward E. Amoroso, CEO, Tag Cyber LLC</b> <ul style="list-style-type: none"><li>– Jeffrey Eisensmith, CISO, DHS OCIO</li><li>– Sara Mosley, Acting Director for the Office of the Chief Technology Officer, DHS CS&amp;C</li><li>– Jack Wilmer, Cyber lead for American Technology Council, White House OSTP</li><li>– Ken Bible, Deputy CIO, U.S. Marine Corps</li></ul>
10:30	<b>Break &amp; Networking</b>
10:45	<b>Standards to Measure and Manage Security, Resilience and Technical Debt</b> <ul style="list-style-type: none"><li>– Dr. Bill Curtis, Executive Director, Consortium for IT Software Quality (CISQ)</li><li>– John Weiler, Vice Chair, IT Acquisition Advisory Council (IT-AAC)</li></ul>
11:25	<b>Cyber Resilience Standards of Practice</b> <b>Lead: Dr. Bill Curtis, Executive Director, Consortium for IT Software Quality (CISQ)</b> <ul style="list-style-type: none"><li>– Dr. Ron Ross, Computer Scientist and Fellow, NIST</li><li>– Roberta Stempfley, Director of SEI's CERT Division</li><li>– Herb Krasner, University of Texas at Austin (ret.), Texas IT Champion</li></ul>
12:15	<b>Luncheon and Networking</b>
12:45	<b>Luncheon Keynote: Defense Cyber Way Forward</b> <ul style="list-style-type: none"><li>– Dr. Thresa Lang, Deputy Director, Navy Cybersecurity/Deputy Director, Department of the Navy Deputy Chief Information Officer (Navy)</li></ul>
1:15	<b>Titans of Cyber Panel: Best Practices and Innovations for Rapid, Secure Modernization</b> <b>Lead: John Weiler, Vice Chair, IT Acquisition Advisory Council (IT-AAC)</b> <ul style="list-style-type: none"><li>– Therese Firmin, Principal Director, DCIO (CS) and Deputy Chief Information Security Officer, Department of Defense</li><li>– Jose Arrieta, Director, Office of IT 70 Schedule Contract Operations, GSA</li><li>– Brigadier General (ret) Greg Touhill, former U.S. CISO; President of Cyxtera Federal Group</li><li>– Matt Conner, CISO, National Geospatial-Intelligence Agency</li></ul>
2:15	<b>Supply Chain and Integration Risk Management</b> <b>Lead: Joe Jarzombek, Global Manager, Synopsys Software Integrity Group</b> <ul style="list-style-type: none"><li>– Emile Monette, Senior Cybersecurity Strategist and Acquisition Advisor, DHS Continuous Diagnostics and Mitigation Program</li><li>– Shon Lyublanovits, IT Security Category Manager and Director of the Security Services Division for the Office of Integrated Technology Services (ITS) in GSA's Federal Acquisition Service (FAS)</li><li>– Dave Duma, Acting Director, Operational Test and Evaluation, Department of Defense</li></ul>

Take note of who at the Federal Level supports CISQ, ongoing software risk assessment?

# Are your State's Mission Critical Applications CISQ Compliant?

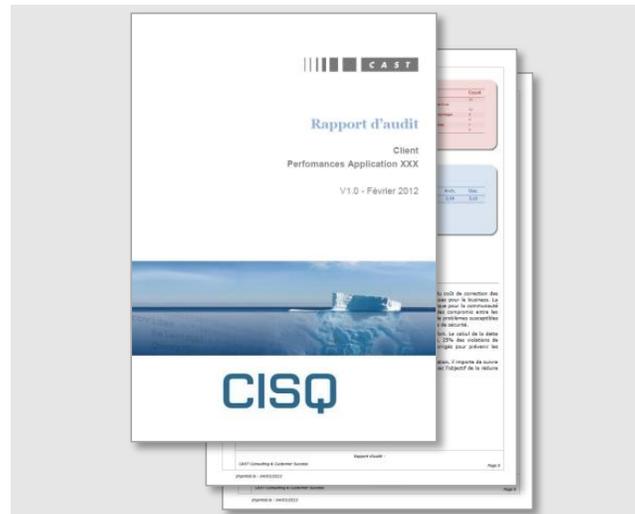


## Quality Certificate



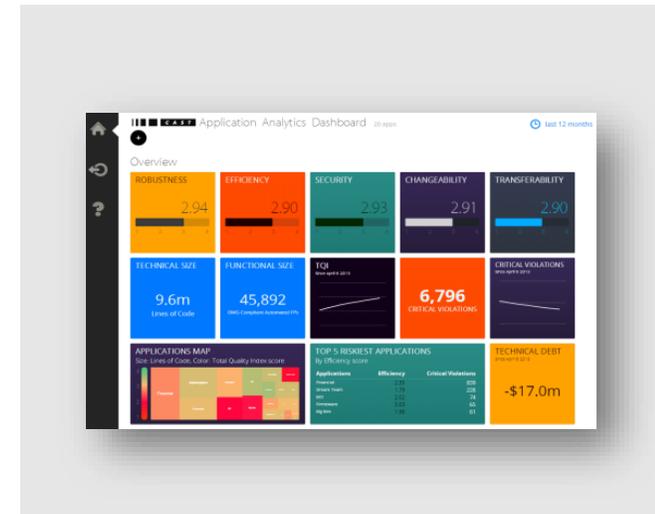
Certifies analysis results adhere to CISQ specifications

## Detailed Analysis Report



Report includes description of rules and statistics of violations

## Analytics Dashboard



Aggregated view of all applications analyzed with the CISQ Assessment Model

**Your NASCIO membership gets your state one complimentary assessment.**

email us at [publicsector@castsoftware.com](mailto:publicsector@castsoftware.com) for details.



# Questions

Marc Jones  
Vice President Public Sector  
[m.jones@castsoftware.com](mailto:m.jones@castsoftware.com)  
703.863.9908  
**Twitter:** @mjo1k



# Follow Us



@NASCIO



/NASCIOmedia



/NASCIOmedia



National Association of State  
Chief Information Officers  
(NASCIO)