Establishing Standards as the Basis for Effective Measurement and Affordability

Marc Jones Federal Director, CISQ (vol.)

marc.jones@it-cisq.org / 703.863.9908

CISQ founders

Carnegie Mellon Software Engineering Institute

OMG OBJECT MANAGEMENT GROUP®

it-cisq.org

CISQ Bottom Line Up Front

- **Legislative attempts to mitigate IT Application quality related risks still fall short**
- **Current emphasis on software level cybersecurity targets only one part of the 'quality' issue – potentially at the expense of other risks that can yield similar outcomes**
- **Pragmatic standards developed with Industry & Federal (Civil & DOD) collaboration are now available to be used by Acquisition, Program Management and IVV.**
- **Standard automated functional sizing measurement exists that can now be used to correlate with existing models and risk management to validate affordability(dev & sustain) work and sprint/release throughput.**

CISQ Existing Legislation Points to Standards…

- **Clinger Cohen Act recognizes that government must leverage commercial IT**

  (1) *Streamline the IT Acquisition Process*

  (2) *Change business processes (BPR), not COTS*

  (3) *Favor COTS/OSS over custom development (GOTS).*

  (4) *Build business case and select based on lifecycle cost and business value*

  (5) ***Adopt Commercial IT Standards of Practices (augmented by OMB A119)***

- **OMB 25 Point Plan Requires: *"Align the Acquisition Process with the Technology Cycle"***

  Point 13. Design and develop a cadre of specialized IT acquisition professionals .

  Point 14. ***Identify IT acquisition best practices and adopt government-wide****.*

  Point 15. Issue contracting guidance and templates to support modular development

  Point 16. Reduce barriers to entry for small innovative technology companies"

- **Federal IT Acquisition Reform Act (FITARA) :**

  1. Agency Chief Information Officer (CIO) Authority Enhancements 2. **Enhanced Transparency and Improved Risk Management in IT Investments 3. Establish Portfolio Review** 4. Federal Data Center Consolidation Initiative 5. Expansion of Training and Use of IT Cadres 6. Maximizing the Benefit of the Federal Strategic Sourcing Initiative 7. Government wide Software Purchasing Program

- **EO13636 Recommends six acquisition reforms:**

  i. *Institute Baseline Cybersecurity Requirements as a Condition of Contract Award for Appropriate Acquisitions*

  ii. *Address Cybersecurity in Relevant Training*

  iii. *Develop Common Cybersecurity Definitions for Federal Acquisitions*

  iv. *Institute a Federal Acquisition Cyber Risk Management Strategy*

  v. *Include a Requirement to Purchase from Original Equipment Manufacturers, Their Authorized Resellers, or Other "Trusted" Sources, Whenever Available, in Appropriate Acquisitions*

  vi. *Increase Government Accountability for Cyber Risk Management*

Source:

CISQ DoD Mandates Software Quality…

2014 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.--

…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

2013 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.

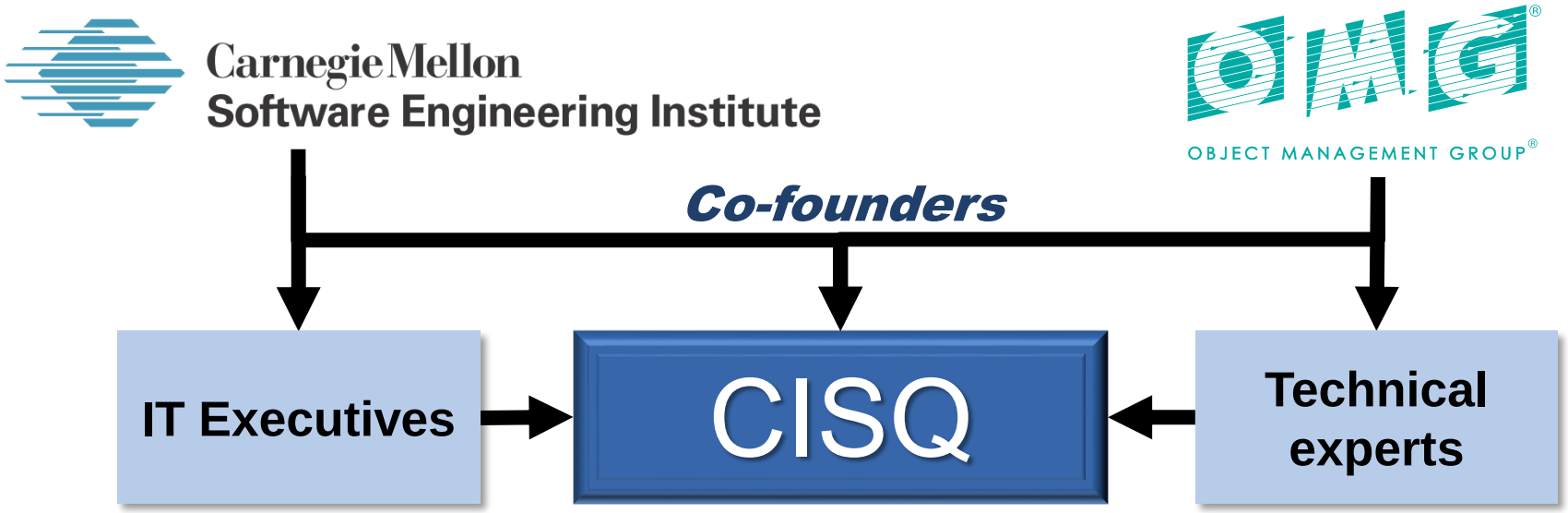
SEC. 933. IMPROVEMENTS IN ASSURANCE OF COMPUTER SOFTWARE PROCURED

BY THE DEPARTMENT OF DEFENSE.

(a) Baseline Software Assurance Policy.--The Under Secretary of

….shall develop and implement a baseline software assurance policy for the entire lifecycle of covered systems….. (4) …promote best practices and standards to achieve software *security, assurance, and quality* …

CISQ What Is CISQ ?



OMG Special Interest Group

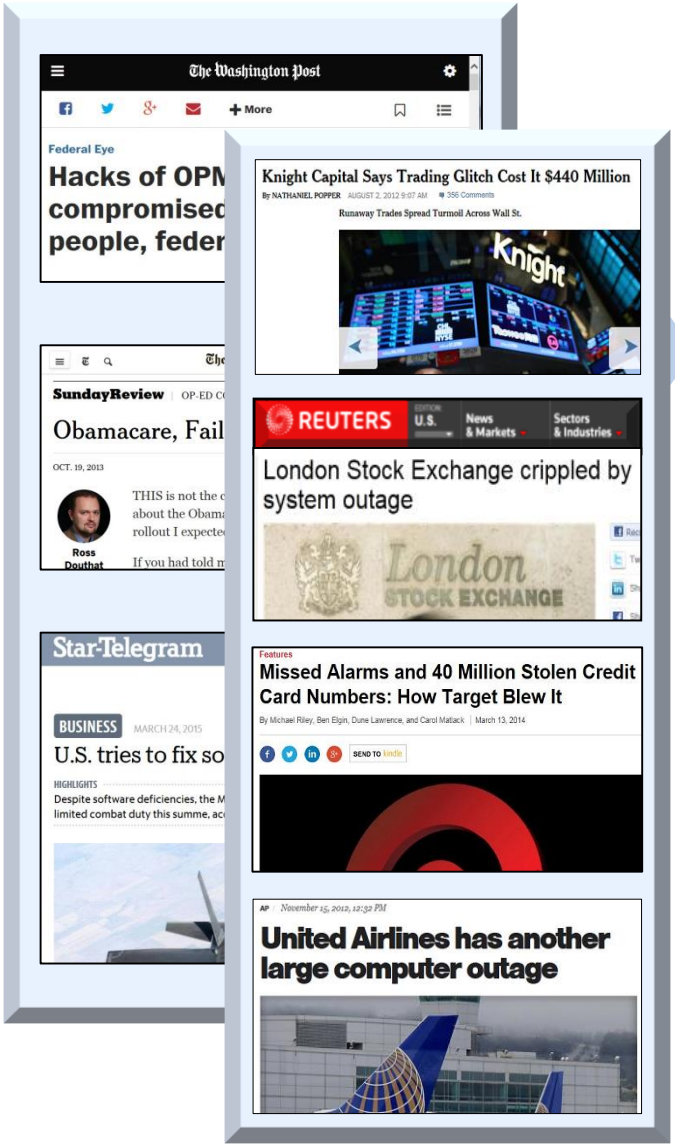
CISQ is a non-profit chartered to define automatable measures of software size and quality that can be measured in the source code, and promote them to become Approved Specifications of the OMG

Current CISQ Sponsors

accenture
Atos
CAST
HUAWEI
WIPRO Applying Thought
Booz | Allen | Hamilton

CISQ Risk broader than Cyber 'security'

Gov – Industry IT disasters



Can impact

POTUS, Cabinet
PEOs, OCIOs, Warfighter

Corporation
Customers
Citizens
Markets

accountable for

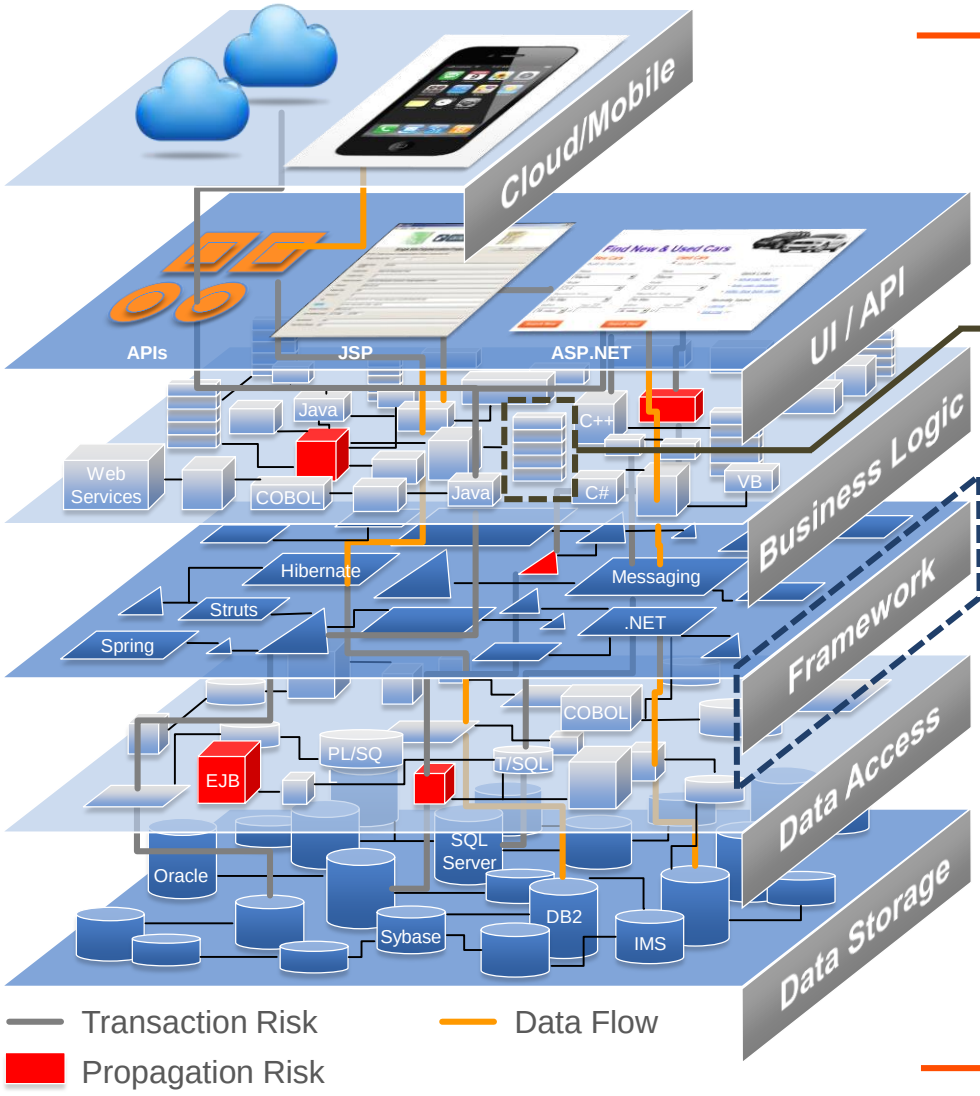
National Security/Critical Infrastructure

Customer/Citizen confidence

Agency/Corporate efficiency

Evaluation of IT System Quality with CISQ Measures

This is a Modern Gov. System…



Code / Unit Level Risk

- Typically open source or cheap IDE/Developer level Code style & layout focus
- Expression complexity
- Code documentation
- Class or program design
- Basic coding standards

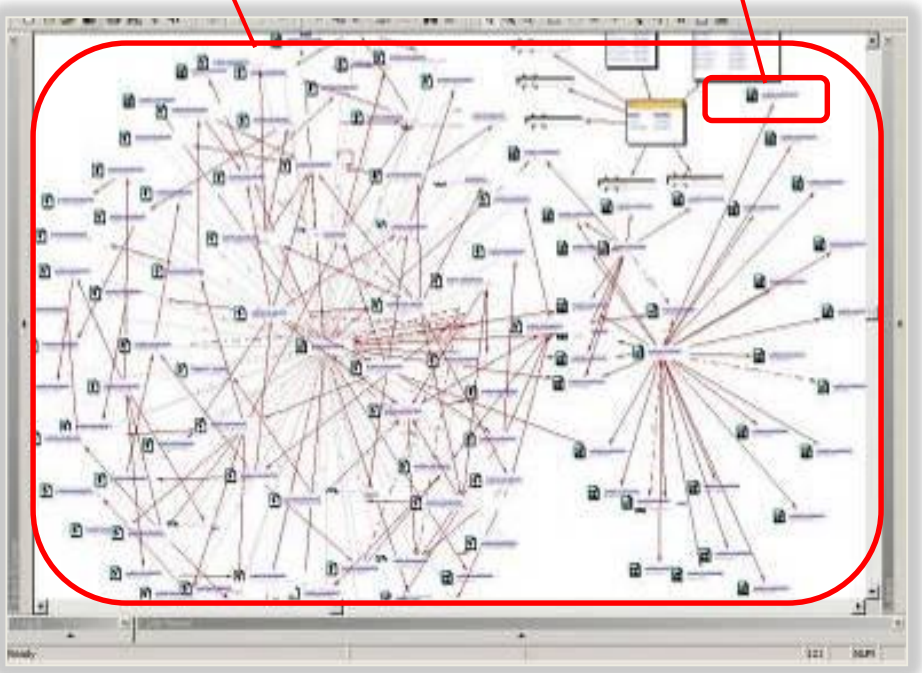
Technology Level Risk

- Single language / technology layer
- Intra-technology architecture
- Intra-layer dependencies
- Design & structure
- Inter-program invocation
- Security vulnerabilities
- Development team level
- Language Specific project tools

CISQ: System Level Enterprise Risk

- Integration quality
- Architectural compliance
- Risk propagation
- Application security
- Resiliency checks
- Transaction Integrity & Security around data access
- Automated Function point - Effort estimation / verification
- Data access control
- Calibration across technologies
- Enterprise Grade Solution Space

CISQ …But Typical QA Points to Code Risk



"If your contractors tell you they are doing code quality, they mean "code" level quality - and they may not even be doing that consistently."

- Fed Director of Enterprise Apps

System Risk

System quality measures how well individual application components work together to make up the overall system – Whether system is a large single language or multi-tiered/ multi-technology.

Code Risk

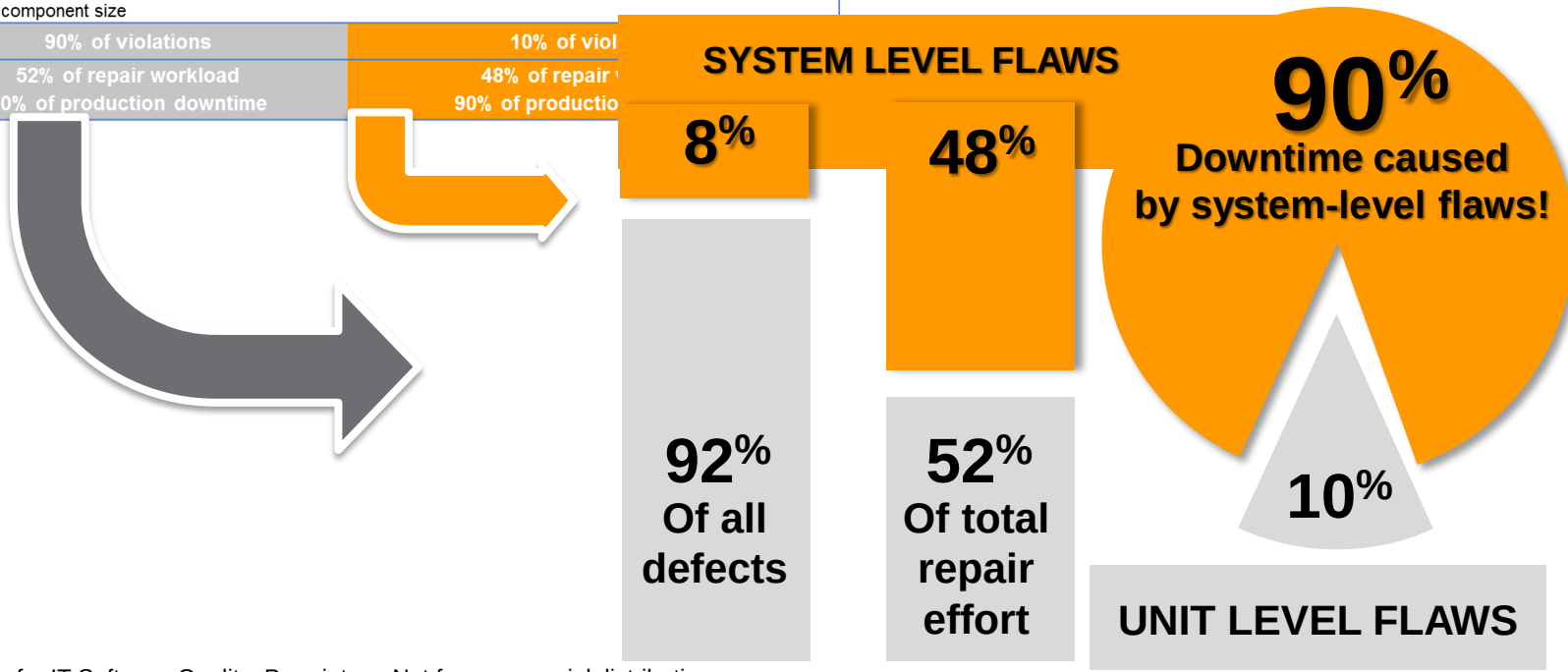
Code quality is the measure of individual components for compliance with standards and best practices in the context of a specific language. These are typically developer tools.

CISQ Need to Measure SYSTEM Level Risk

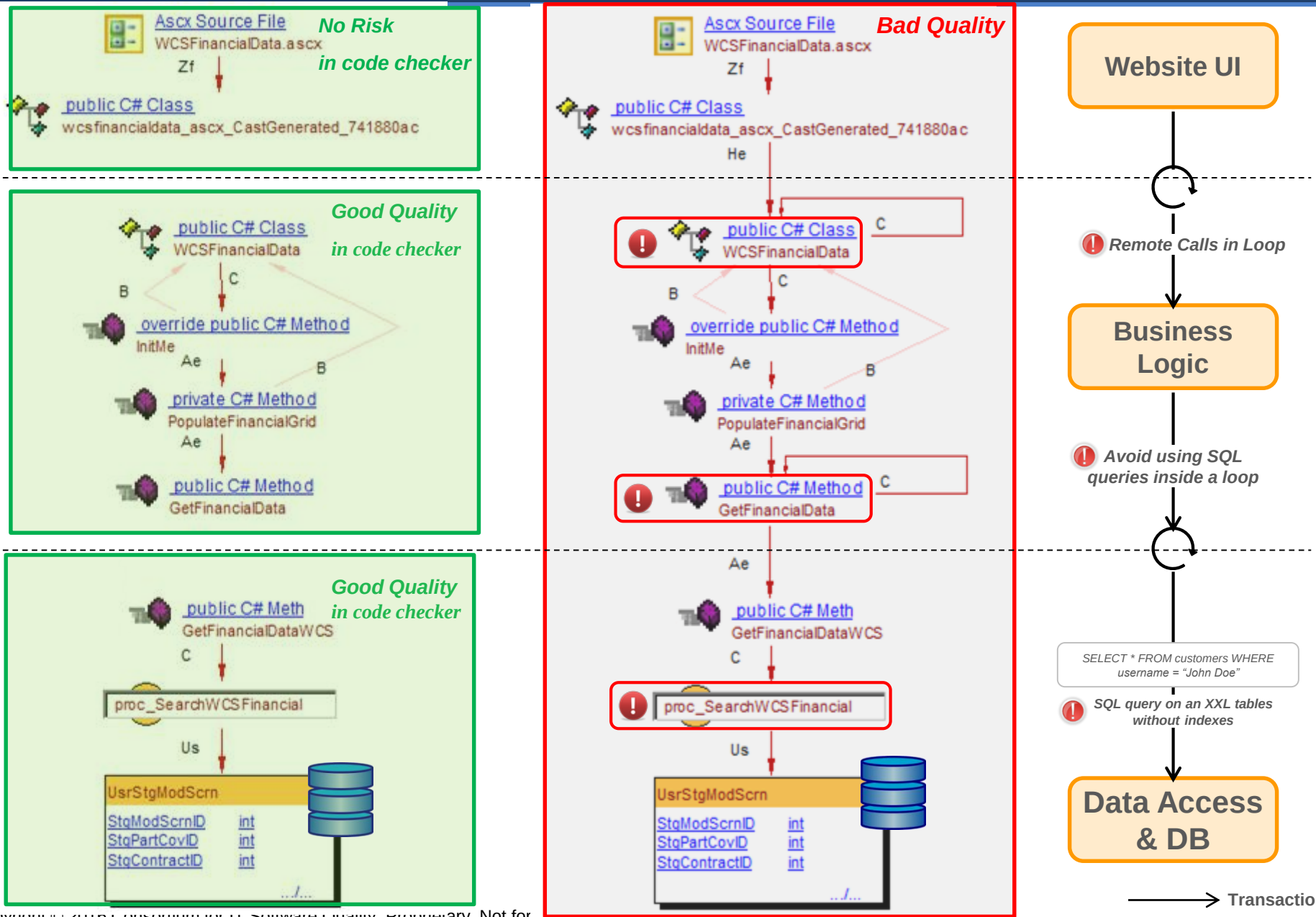
Business Characteristic	Good Coding Practices @ Unit-Level	Good Architectural Practices @ Technology/System Levels
RELIABILITY	Protecting state in multi-threaded environments Safe use of inheritance and polymorphism Resource bounds management, Complex code Managing allocated resources, Timeouts	Multi-layer design compliance Software manages data integrity and consistency Exception handling through transactions Class architecture compliance
PERFORMANCE EFFICIENCY	Compliance with Object-Oriented best practices Compliance with SQL best practices Expensive computations in loops Static connections versus connection pools Compliance with garbage collection best practices	Appropriate interactions with expensive or remote resources Data access performance and data management Memory, network and disk space management Centralized handling of client requests Use of middle tier components vs. procedures/DB functions
SECURITY	Use of hard-coded credentials Buffer overflows Missing initialization Improper validation of array index Improper locking Uncontrolled format string	Input validation SQL injection Cross-site scripting Failure to use vetted libraries or frameworks Secure architecture design compliance
MAINTAINABILITY	Unstructured and duplicated code High cyclomatic complexity Controlled level of dynamic coding Over-parameterization of methods Hard coding of literals Excessive component size	Duplicated business logic Compliance with initial architecture design Strict hierarchy of calling between architectural layers Excessive horizontal layers Excessive multi-tier fan-in/fan-out
NUMBER OF ISSUES	90% of violations	10% of viol
BUSINESS IMPACT	52% of repair workload 10% of production downtime	48% of repair 90% of productio

"Tracking programming practices at the Unit Level alone may not translate into the anticipated business impact… most devastating **defects can only be detected at the System Level."**

OBJECT MANAGEMENT GROUP®



CISQ System-level defects visible in a transaction



CISQ Focus on Attributes With Highest Impact

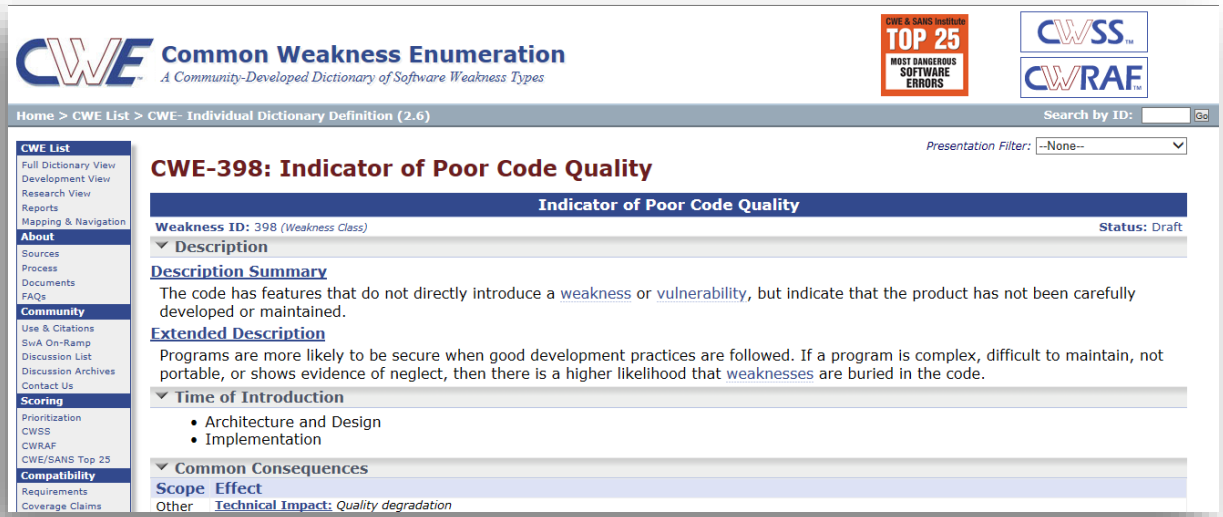
CISQ Quality Characteristic Measures

Outcomes

Security	Ability to prevent unauthorized intrusions and data theft	National Security, fraud, trust, damages
Reliability	Ability to avoid outages and to recover operations quickly	Mission effectiveness, citizen satisfaction
Performance Efficiency	Ability to avoid response degradation, resource overuse	Mission effectiveness, cost, satisfaction
Maintainability	Ability to understand and modify software quickly	Cost of ownership, agility, time to mission

http://it-cisq.org/standards/automated-quality-characteristic-measures

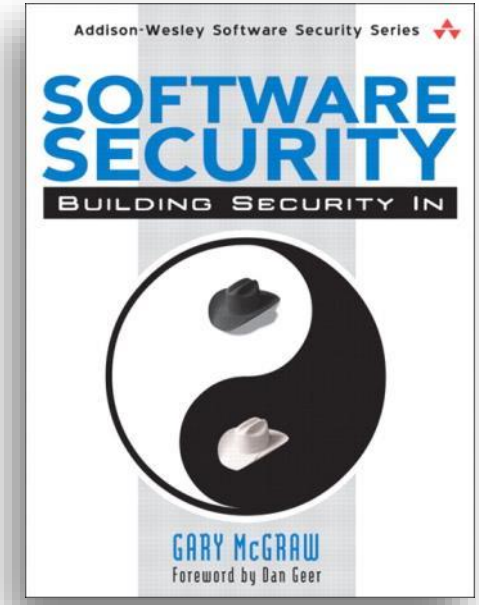
CISQ "System Risk" Includes Security Assurance



Architecture & Quality Attributes are now components of Common Weakness & STIGS

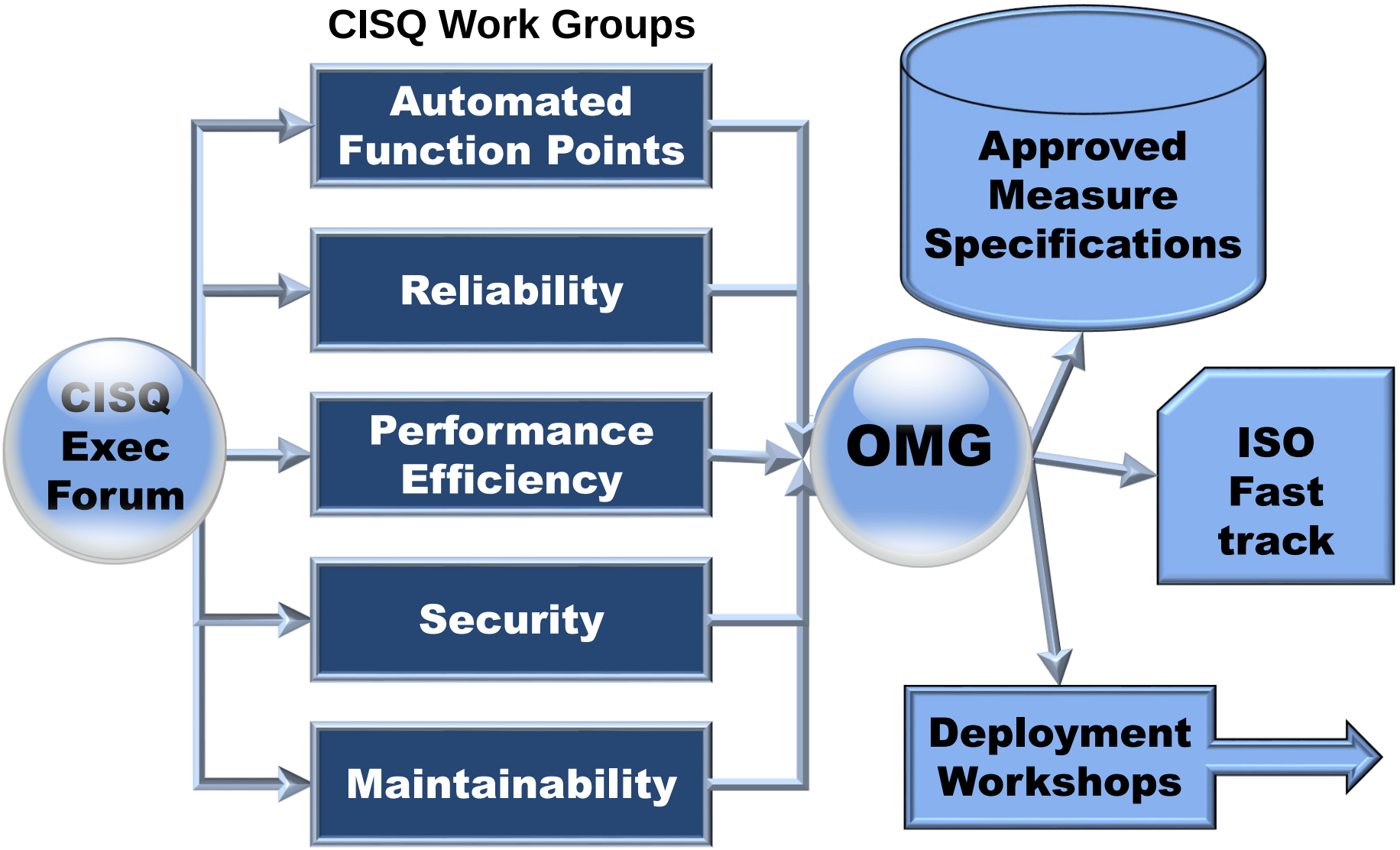
"30-50% of software level security findings are in 'dead' code or in code so fundamentally flawed it should not be secured, but re-factored." - OMG Roundtable Survey, March 2014

"More than 50% of security problems have their root cause in structural quality flaws." - Gary McGraw



OMG
WE SET THE STANDARD

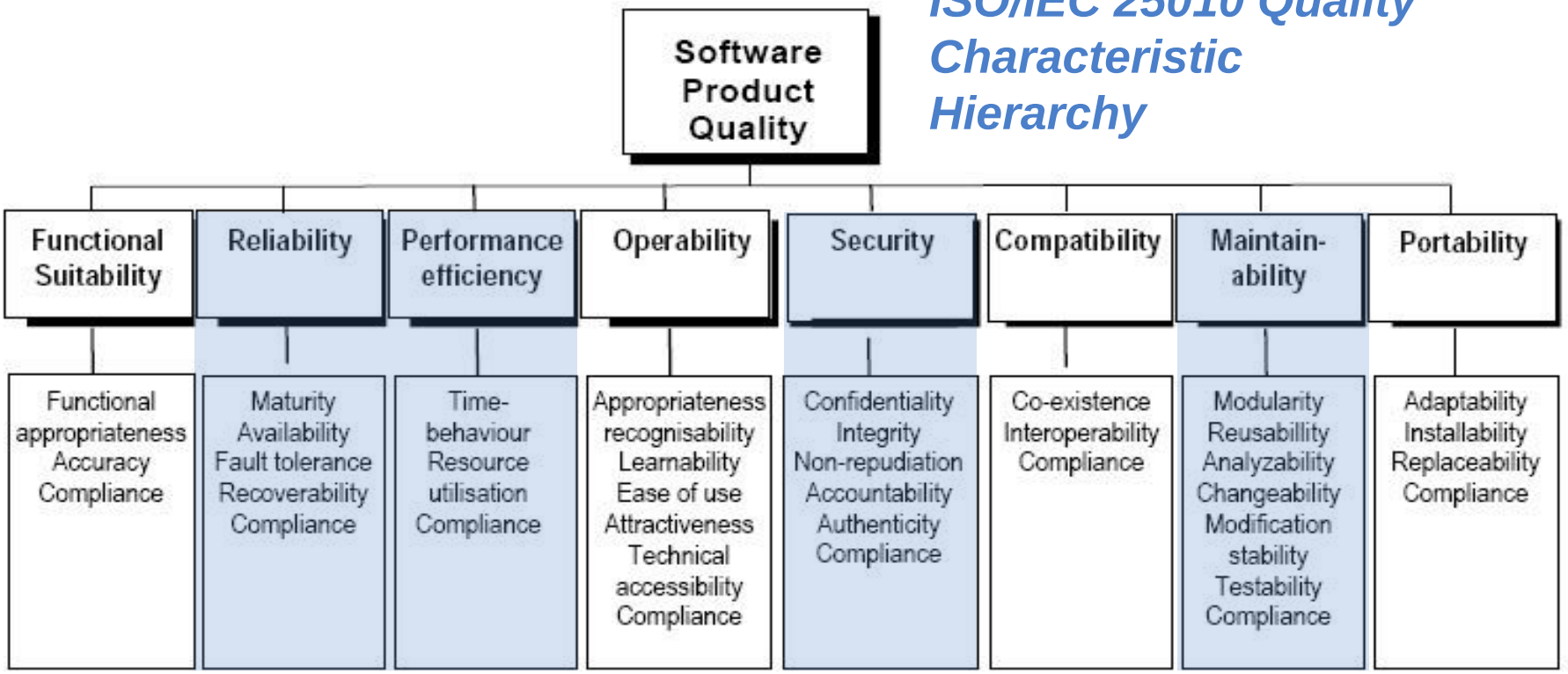
CISQ/OMG Standards Process



CISQ How Do CISQ Measures Relate to ISO?

- **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**

ISO/IEC 25010 Quality Characteristic Hierarchy

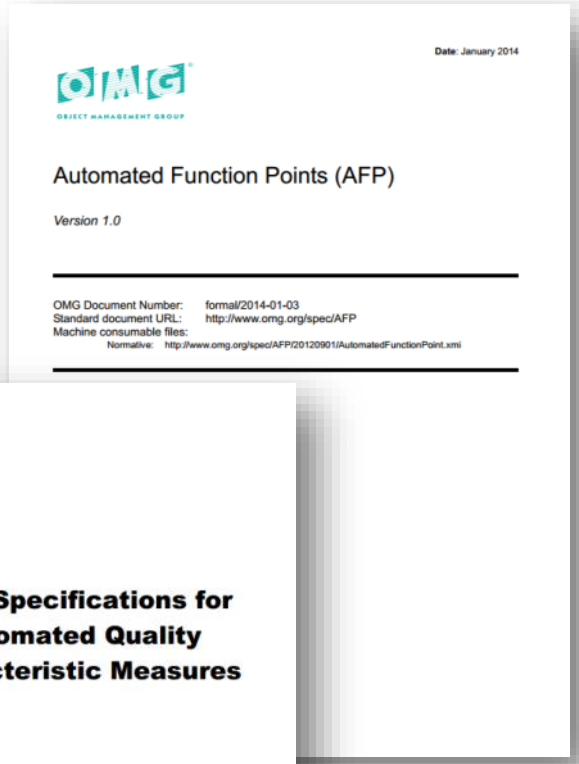


CISQ defined automatable measures for quality characteristics highlighted in blue

CISQ Standards of Measurement Supported by FFRDCs, Government, Industry

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.

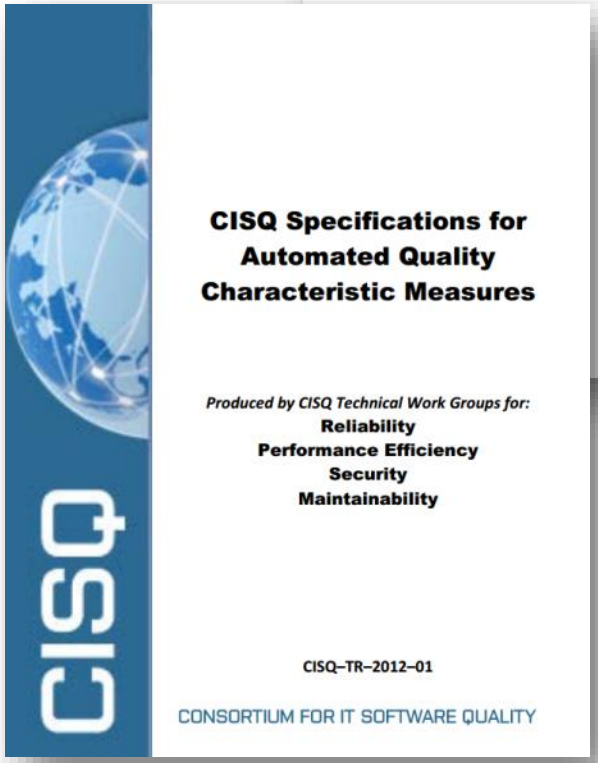


Object Management Group (OMG)

- 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)

Consortium for IT Software Quality (CISQ)

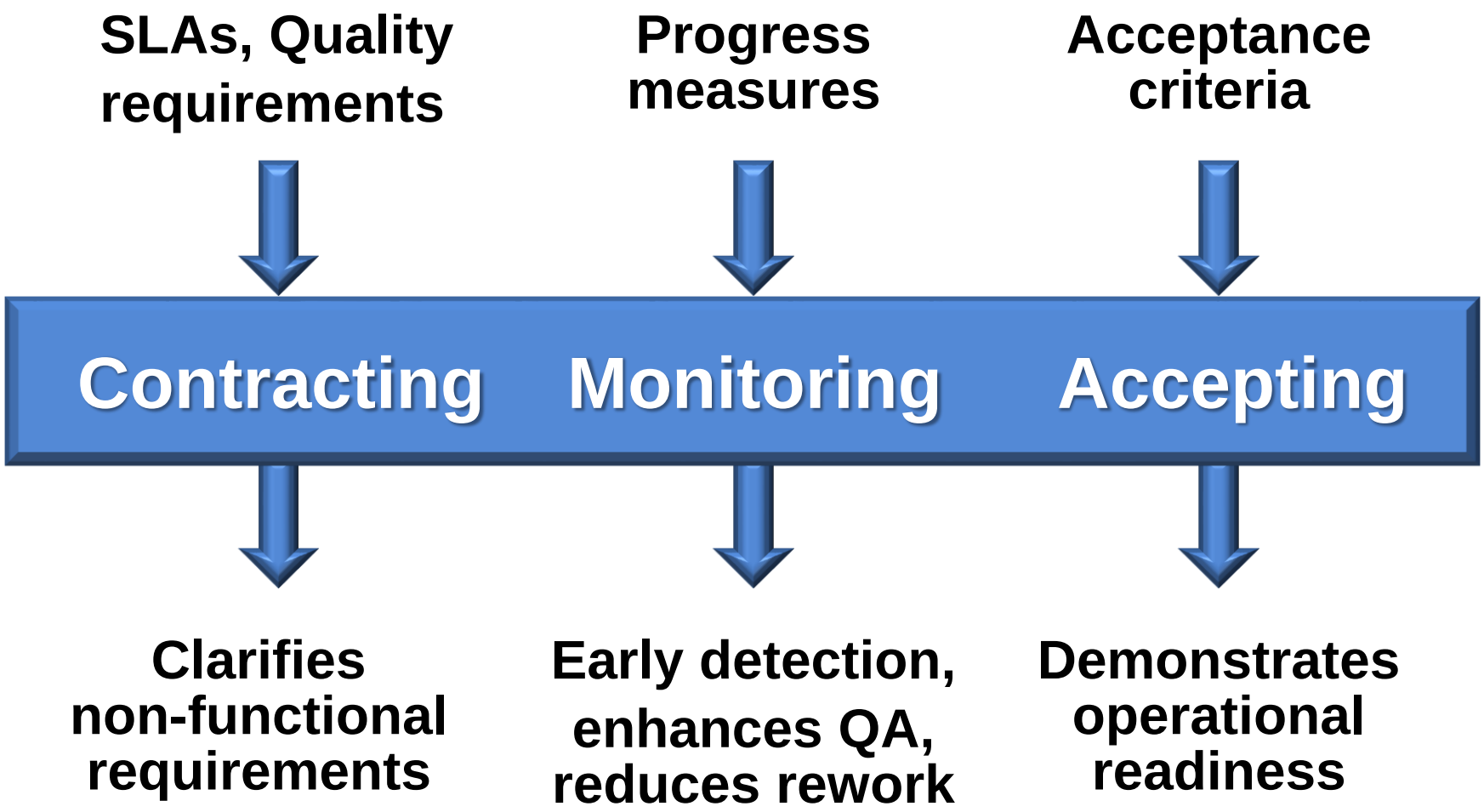
- Goal:
  - Improve IT application quality
  - Reduce cost and risk
- Objective is to introduce a **computable metrics standard** for measuring **software quality & size**
- IT executives from Global 2000, system integrators, outsourced service providers, and software technology vendors



Software Engineering Institute

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

CISQ Need to Leverage in Federal Acquisition



- **Now let's discuss Automated Sizing Standards**
- **(Presentation slide removed)**

Looking Beyond SLOC (2014 SBIR example)

N141-055 TITLE: Automated Function Point Analysis

TECHNOLOGY AREAS: Information Systems

ACQUISITION PROGRAM: PEO IWS 1.0, Integrated Combat Systems, AEGIS

OBJECTIVE: Develop an innovative function point analysis software tool for program managers that achieves requirements for estimating software costs.

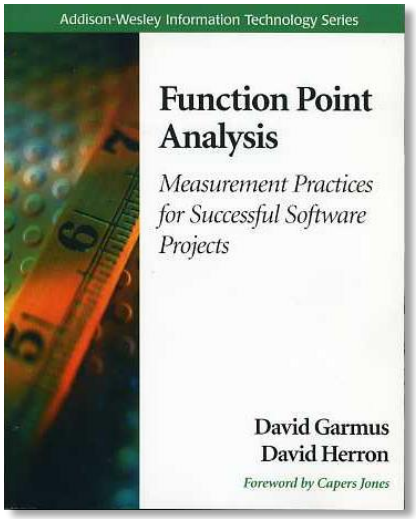
DESCRIPTION: The Navy uses estimates of software size such as Source Lines of Code (SLOC)) to determine software development efforts and their associated combat system development costs. There are significant variations in methods used for estimating SLOC, which introduce risk. Current SLOC estimates are a prediction of end-product code size that varies with code language (such as Java, C++) and software design approach. Estimates of new, modified, and reused SLOC to implement a capability are based upon a Subject Matter Expert's (SME) judgment which makes the resulting estimate highly subjective (Ref 1).

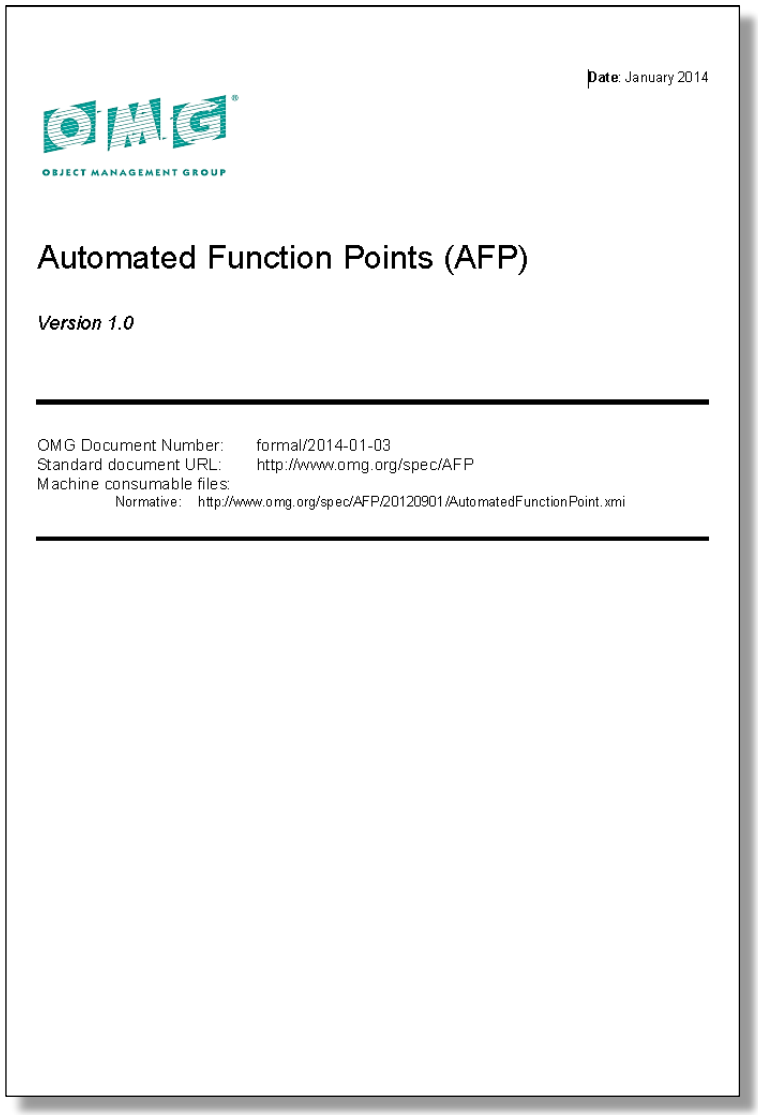
Program Managers are required to prevent program cost overruns. They rely upon accurate cost estimates and software development metrics to ensure programs are executable and not at risk of cost overruns. The use of SLOC creates high risk cost estimates due to the potential for significant variation in methods for estimating end-product source lines of code.

The International Function Point User Group (IFPUG) has developed a Function Point based methodology to estimate software costs that is more accurate than the SLOC methodology. The Navy's transition to the Function Point based methodology has been hindered because existing historical cost data is based upon SLOC. Significant manual effort is needed to transition from the current Navy SLOC practice to the current industry Function Point methodology. The Object Management Group (OMG) recently adopted an Automated Function Point (AFP) Specification. The standard defines how to count function points that can be used to ensure software counting consistency and will provide the standard required to enable transition from SLOC to Function Point based software estimation methodologies (Ref 2, 3). However

CISQ Automated Function Points

- **An OMG Approved Specification**
- **Mirrors IFPUG counting guidelines, but automatable**
- **Specification developed by international team led by David Herron of David Consulting Group**
- **Growing commercial adoption**





Date: January 2014

OBJECT MANAGEMENT GROUP

Automated Function Points (AFP)

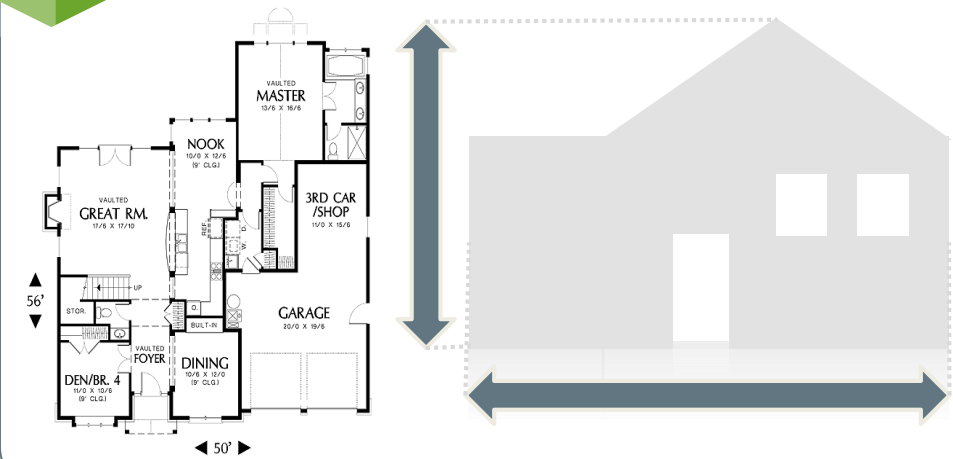
Version 1.0

OMG Document Number: formal/2014-01-03
Standard document URL: http://www.omg.org/spec/AFP
Machine consumable files:
Normative: http://www.omg.org/spec/AFP/20120901/AutomatedFunctionPoint.xmi

http://it-cisq.org/standards/automated-function-points

CISQ Automated Function Points Defined

AFP Application Function Points



Automated Function Points is a technology agnostic metric, independent on the complexity and the quality.

Measure the number of transaction manage by the application in order to measure the amount of functionality.

Best used for overall functional size of application (Used on Run the Business)

EFP Enhancement Function Points

Enhanced Function Points is a functional sizing unit that measures application enhancements and maintenance activities.

Measure the number of modifications (added, updated, deleted) between two measurements.

Best used to show changes (Add/Delete/Change) in releases

CISQ Software Sizing: Industry Use Case Profiles

Standardized & Benchmarking

Detect portfolio outliers, identify improvement opportunities and track evolution of size, risk, complexity and quality

IT focus: Productivity Measurement & Improvement

Monitor, track and compare ADM teams' utilization, delivery efficiency, throughput and quality of outputs

CLIENT NAMES REMOVED

Business focus: Quantify Effectiveness of Transformation Initiative

Optimize operating costs while preserving throughput and de-risking business transformation initiative

ADM Supplier Outcome Measurement

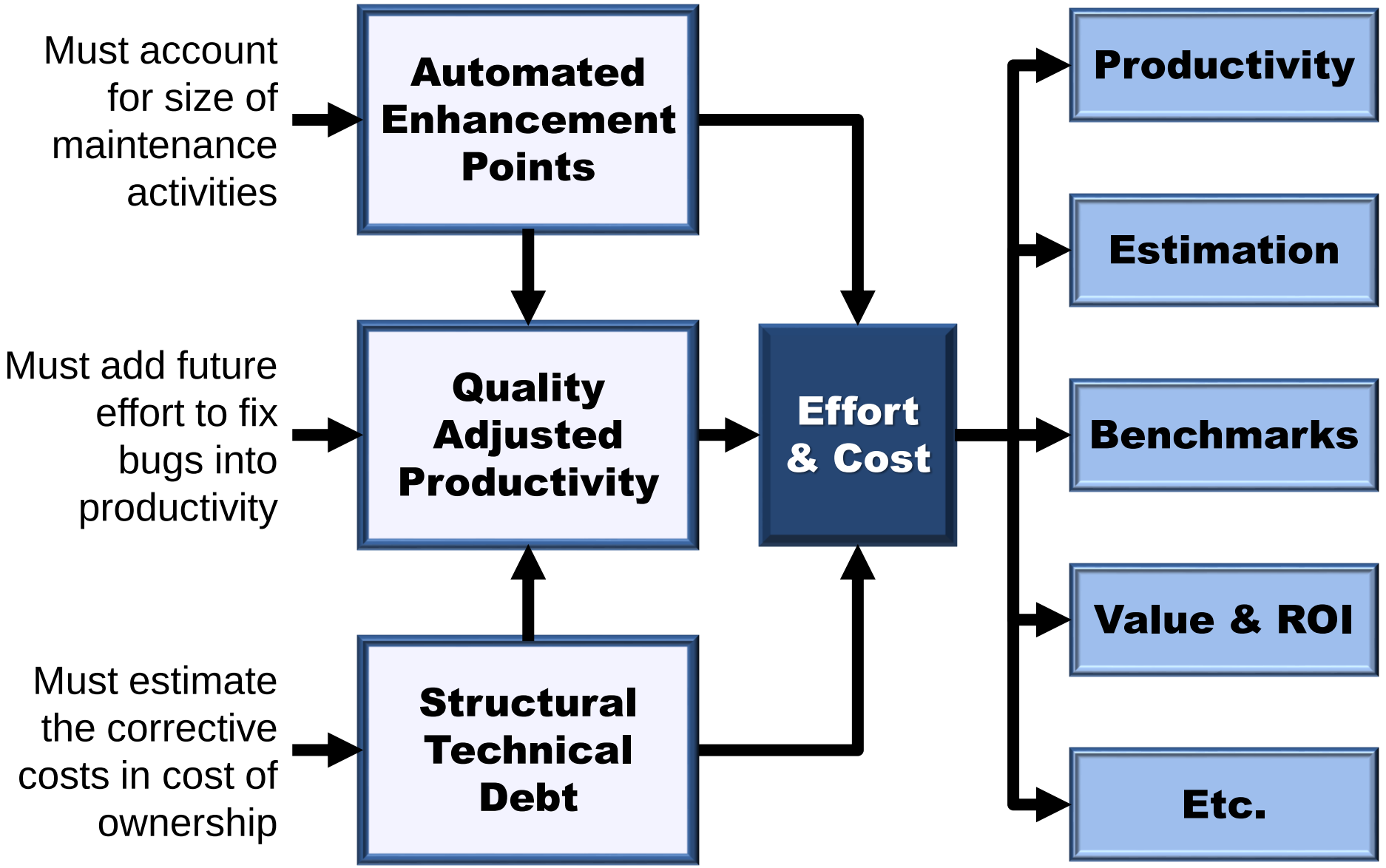
Provide visibility to management; manage risk, quality and throughput through enhanced Service Level Agreement

CLIENT NAMES REMOVED

Industry Use Case Slides

- **Removed**

CISQ New CISQ Measures



CISQ Event March 15, 2016 www.it-cisq.org

Phyllis Schneck
Deputy Under Secretary for Cybersecurity and Communications for the NPPD, Department of Homeland Security

Curtis Dukes
Director of Information Assurance, National Security Agency

Lucia Savage
Chief Privacy Officer, Office of the National Coordinator or Health Information Technology, Department of Health & Human Services

Dr. J. Michael Gilmore
Director of Operational Test and Evaluation, Office of the Secretary of Defense, Department of Defense

Paul Nielsen
Director and CEO, Software Engineering Institute at Carnegie Mellon University

CISQ Event Schedule for March 15, 2016

9:00am	**Titans of Cyber Panel: Critical Insights from the Front Lines of the Cyber Risk Management Battle** - Phyllis Schneck, Deputy Under Secretary for Cybersecurity and Communications for the National Protection and Programs Directorate (NPPD), U.S. Department of Homeland Security - Curtis Dukes, Director of Information Assurance, National Security Agency - Lucia Savage, Chief Privacy Officer, Office of the National Coordinator for Health Information Technology, U.S. Department of Health & Human Services - Dr. J. Michael Gilmore, Director of Operational Test and Evaluation (OT&E), Office of the Secretary of Defense, U.S. Department of Defense - Paul Nielsen, Director and CEO, Carnegie Mellon SEI - Luke McCormack, CIO, U.S. Department of Homeland Security (invited)
10:30am	**Refreshment Break**
10:45am	**Ensuring the Resiliency of Software-Intensive Systems** - Dr. Bill Curtis, Executive Director, CISQ - David Zubrow, Senior Member of the Technical Staff, Carnegie Mellon SEI - Dr. Vadim Okun, Computer Scientist, National Institute of Standards and Technology (NIST) - Kris Britton, Director, NSA Center for Assured Software - Dr. Robert Childs, Chairman, Technology Committee, Armed Forces Communications and Electronics Association
11:30am	**Certifying Software Against CISQ Automated Quality Measures** Dr. Bill Curtis, Executive Director, CISQ
12:00pm	**Lunch**
1:00pm	**Executive Order 13636 and FITARA: Empowering CIOs to Drive Down Cyber Risk** - John Weiler, Vice Chair, IT-AAC - Richard Spires, CEO, Resilient Networks, former CIO, U.S. Department of Homeland Security - Tony Scott, Federal CIO, Office of Management and Budget (invited) - Michael Hermus, CTO, U.S. Department of Homeland Security - Honorable Peter Levine, Deputy Chief Management Officer, U.S. Department of Defense (invited)
2:00pm	**IT Acquisition Workshop: How to Write Risk Management and Cyber Resilience Requirements into Contracts** Joe Jarzombek, Global Manager, Software Supply Chain Management, Synopsys Software Integrity Group, former Director for Software & Supply Chain Assurance, U.S. Department of Homeland Security
2:30pm	**Refreshment Break**
2:45pm	**IT Acquisition Workshop: How to Demonstrate Compliance with FITARA and Federal Directives** Joe Jarzombek, Global Manager, Software Supply Chain Management, Synopsys Software Integrity Group, former Director for Software & Supply Chain Assurance, U.S. Department of Homeland Security
3:15pm	**Case Study: Managing Cyber Risk from Development to Deployment**
4:00pm	**Networking Reception**

THANK YOU!!

Marc Jones Federal Director, CISQ (vol.)

marc.jones@it-cisq.org / 703.863.9908

CISQ founders

Carnegie Mellon
Software Engineering Institute

OMG
OBJECT MANAGEMENT GROUP®

it-cisq.org