CISQ

CONSORTIUM FOR IT SOFTWARE QUALITY

The Consortium for IT Software Quality

Dr. Richard Mark Soley
Chairman and CEO
Object Management Group, Inc.

Software Engineering Institute | Carnegie Mellon

OMG OBJECT MANAGEMENT GROUP

A Story from My Hometown

- Great Baltimore Fire of 1904
- Response from Philadelphia, Washington, New York, Virginia, Atlantic City… hundreds of firefighters
- Burned two days, 55 hectares

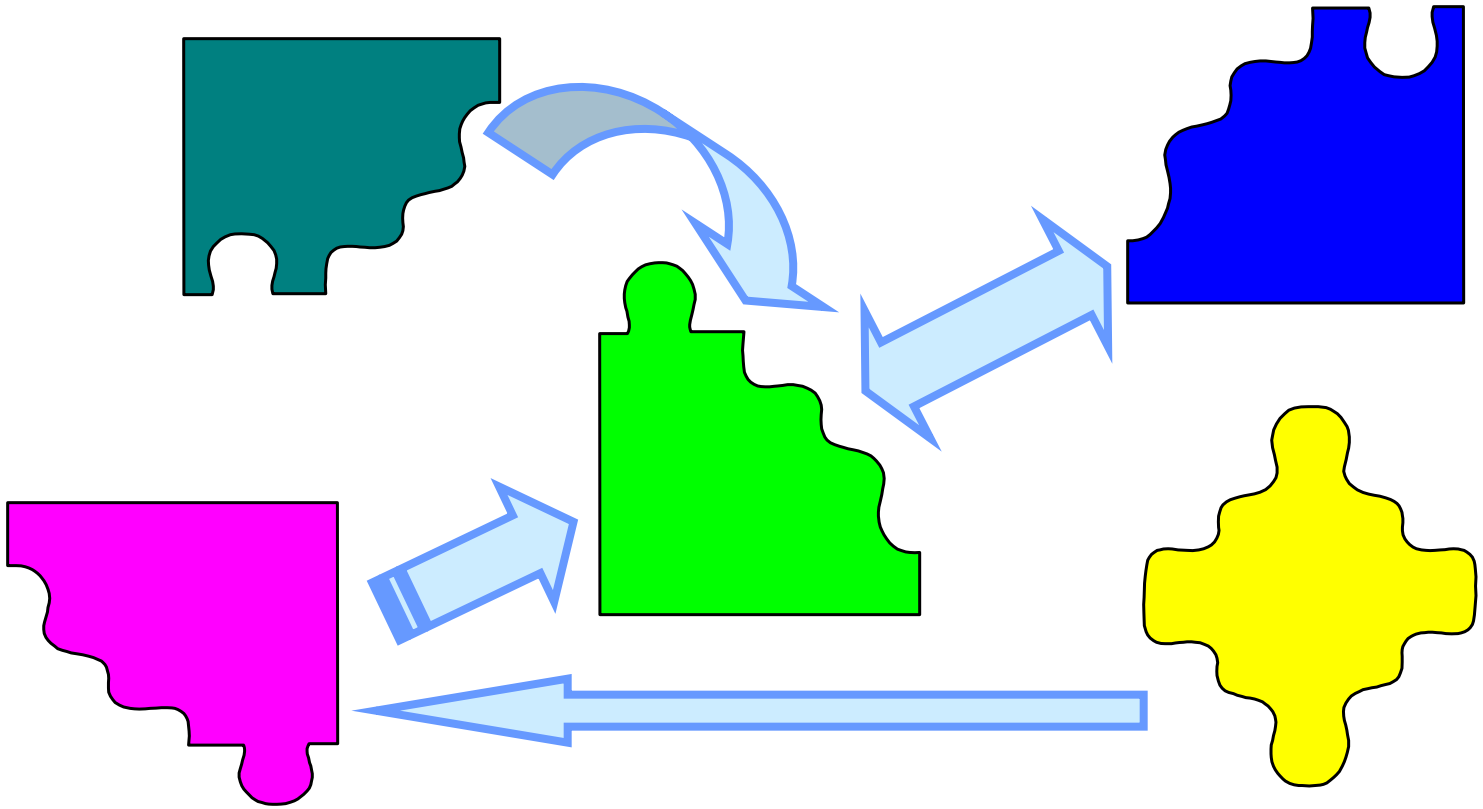
Standards Are Important

- **Sometimes they have life-or-death consequences**
- **Successful standards start, maintain and build ecosystems & businesses**
- **Standards are product differentiators:**
  - Marks of quality
  - Expertise (certification, validation)
  - Interoperability, Portability & Reuse

Heterogeneity is Permanent

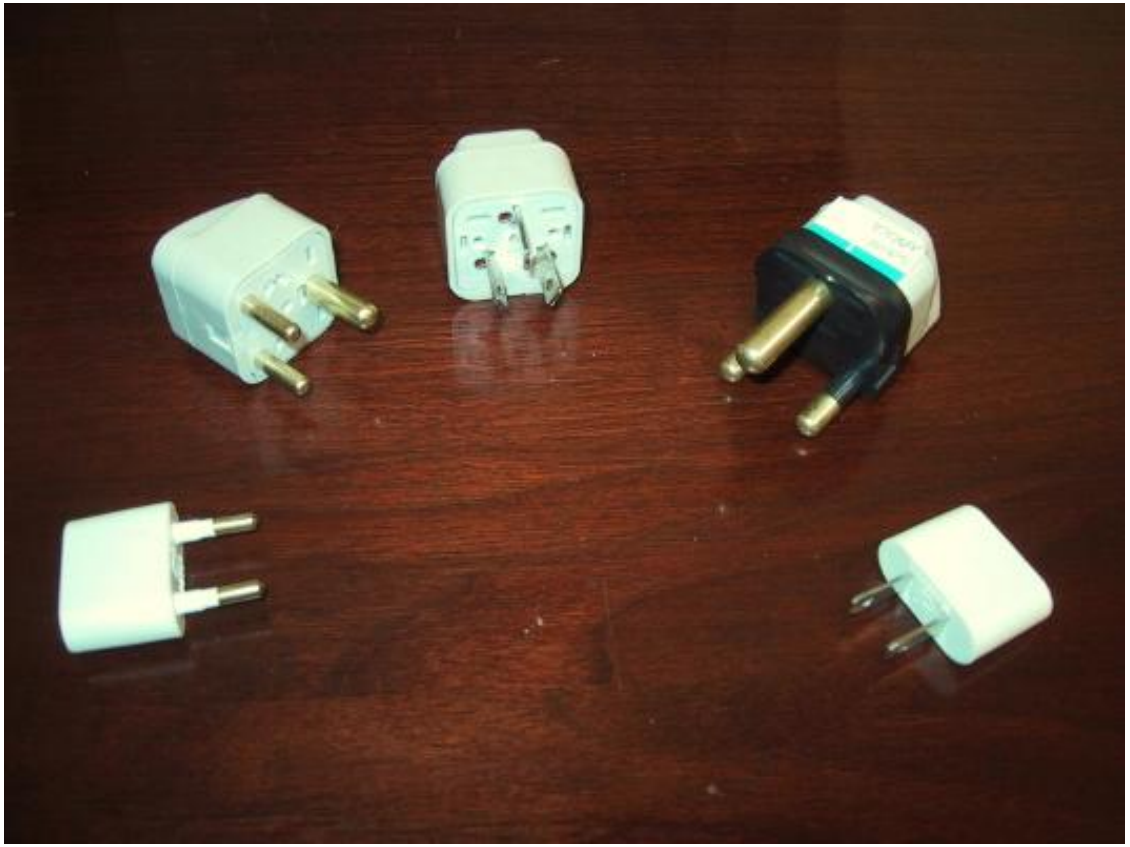
- **Programming languages**
  - ~3 million COBOL programmers
  - ~1.6 million VB programmers
  - ~1.1 million C/C++ programmers
- **Operating systems**
  - Unix, MVS, VMS, MacOS, Windows (all 8!), PalmOS…
  - Windows 3.1: it's still out there!
  - Embedded devices (mobile, set-top, etc.)
- **Networks**
  - Ethernet, ATM, IP, SS7, Firewire, USB
  - Bluetooth, 802.11b, HomeRF

The integration picture is always changing



Executive decisions, mergers & acquisitions have a way of surprising us…

Bringing Down Cost of Adaptation



OMG's Mission Since 1989

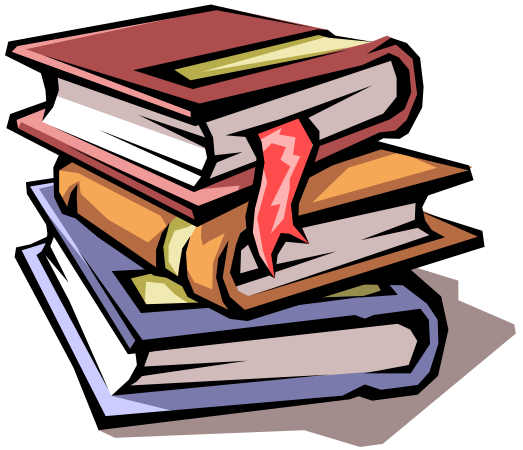
- **Develop an architecture, using appropriate technology, for modeling & distributed application integration, guaranteeing:**
  - reusability of components
  - interoperability & portability
  - basis in commercially available software
- **Specifications *freely available***
- **Implementations exist**
- **Member-controlled not-for-profit**

Who Are OMG?

Adaptive
AIST
Boeing
CA
CSC
DND Canada
DoD OSD
DSTO Australia
Fujitsu
GCHQ
Harris
Hewlett Packard
Hitachi
IBM
Johns Hopkins U.
Mayo Clinic
Microsoft
MITRE
NASA
National Archives
NEC
NIST
NTT DoCoMo
Northrop Grumman
OASIS
Oracle
Penn National Ins.
PRISM
Progress
Sandia Laboratories
SAP
Siemens
Software AG
Software Partners
U. S. Navy SWC
Unisys
VHA
Visumpoint
W3C
Zeligsoft

OMG's Best-Known Successes

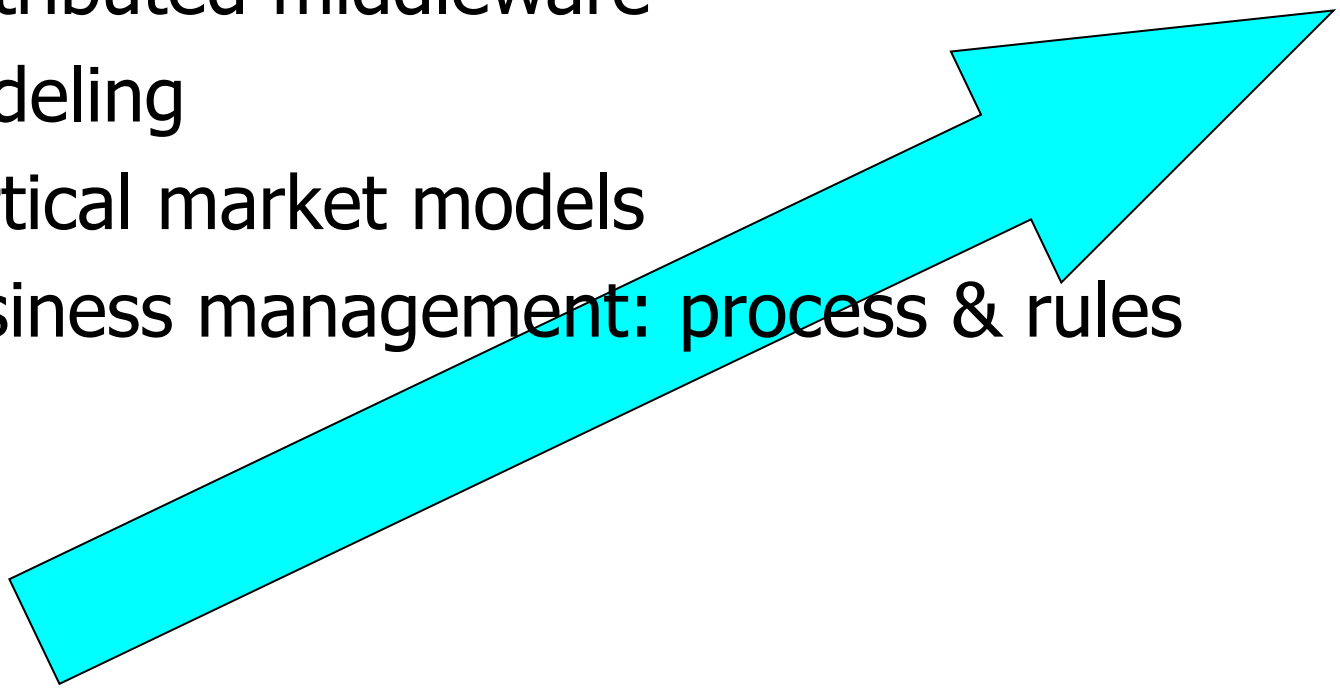
- **Common Object Request Broker Architecture**
  - CORBA® (and the DDS™ Publish/Subscribe model) remains the only language- and platform-neutral interoperability standard
- **Unified Modeling Language**
  - UML® the world's mostly widely adopted standard modeling language
- **Common Warehouse Metamodel**
  - CWM™, the integration of the last two data warehousing initiatives
- **Business Process Modeling Notation**
  - BPMN™ widely adopted for business analysis
- **Meta-Object Facility**
  - MOF™, the language-defining language
- **XML Metadata Interchange**
  - XMI™, the XML-UML standard



Liaison Relationships

Going "Up The Stack"

- **OMG's history has been to address the "technology stack" from the bottom up:**
  - Object orientation
  - Distributed middleware
  - Modeling
  - Vertical market models
  - Business management: process & rules



Modeling is the Focus

- **Modeling, especially graphical modeling is**
  - A natural human approach to design
  - Thousands of years old
  - Allows expression of design separate from implementation, as implementations change
  - Allows for long-term maintenance & integration
  - Is an *accelerator* of implementation
  - Is technology-independent

18th century B.C. multiplication table

The Model Driven Architecture

- **OMG's *Model Driven Architecture* (MDA™) initiative is aimed precisely at modeling "up and down the stack"**
- **You have an opportunity to increase your bottom line by *integrating your assets***
- **Industry standards support that goal by future-proofing your application design**
- **The MDA will help you integrate the mix you have today, and give you an architecture to support the unexpected**
- **Focus on integrating legacy applications**
- **Ensure smooth integration of COTS applications**
- **Models are *testable* and *simulatable***
- **The aim: *a 20-year software architecture***

Shared Languages are Important

- **The Unified Modeling Language is the successor to the dozens of OO A&D notations of the early '90s**
- **UML is broadly adopted, as are other key OMG modeling languages: *BPMN*, SysML, CWM, MOF, XMI**
- **Initial UML 1.x standardized in 1997**
- **Vendor-neutral worldwide certification easily available**
- **Standardization primed the market**
  - Hundreds of books
  - Dozens of commercial tools
  - Widely available training

- **Supported by an open process**
  - UML 2.0 updates came from 54 companies

OMG's Breadth of Standards

- **Besides key modeling, distributed computing & realtime/embedded standards, OMG develops standards in**

Healthcare	Financial Services	Telecommunications
Government	Command & Control	Manufacturing
Robotics	Systems Engineering	Military Communications

25 in all, with new areas including energy systems coming

Gartner on BPM

- **Gartner 2009 worldwide CIO survey: top three CIO priorities are**
  - Business process improvement
  - Reducing enterprise costs
  - Improving enterprise workplace effectiveness

- **"By 2013, graphical models of processes, data, services, user experiences and workflow will be used in more than 80% of new compositions."**
- **"Big Breakthrough: Model-Driven Business"**

Janelle Hill, Gartner (February 2009)

BPM/SOA Community of Practice

- **The BPM/SOA CoP is**
  - An *advocacy group* helping CIO's and line-of-business managers make the transition to BPM, with the support of SOA
  - A *community of practice* helping architects share best practices, success & failure stories

SOA CONSORTIUM™

OMG OBJECT MANAGEMENT GROUP

BPM/SOA Community of Practice

- **The BPM/SOA CoP is**
  - An *advocacy group* helping CIO's and line-of-business managers make the transition to BPM, with the support of SOA
  - A *community of practice* helping architects share best practices, success & failure stories

BPM/SOA™
COMMUNITY OF PRACTICE

Building Ecosystems

BPM/SOA™
COMMUNITY OF PRACTICE

GCIO
COMMUNITY OF PRACTICE™

EVENT PROCESSING COMMUNITY OF PRACTICE™

CYBER SECURITY™
COMMUNITY OF PRACTICE

OMG
OBJECT MANAGEMENT GROUP

Future of the IT Department

- **The successful 21st century organization will no longer have an « IT » department**
- **IT's success means moving from « partnership » and « alignment » to *an integral part of the business organization***
- **Our role: *recognizing, precisely defining, capturing, storing, reusing and* optimizing *business processes***
- **Removing waste: take out the trash!**
- **Optimization is a precursor to** *innovation*

Introducing Business Ecology

- **Business Ecology Initiative recognizes that**
  - IT as a support organization is a dead-end and short-term solution
  - The IT organization must evolve into part of (not just a partner of) the business, with a focus on minimizing waste across all processes that implement business capabilities
  - No-one knows more about the operations of the *whole business* than the IT organization, so…

Introducing Business Ecology

- **…the IT organization of the future will be the key focus of business process**
  - Definition
  - Governance
  - Reuse
  - Optimization

BEI BUSINESS ECOLOGY INITIATIVE

Business Ecology Initiative

- **The Business Ecology Initiative has the mission to**
  - Move the industry to successfully developing & using Business Ecology precepts to deliver Actionable Architectures for optimizing the enterprise
  - Help organizations adopt Business Ecology and develop and implement Actionable Architectures
  - Gain experience by sharing experiences with like-minded organizations making the same transition

Some Major OMG Directions

- **Cloud computing**
  - Cofounded cloudstandards.org; focused on *portable deployment* to support many business models
- **Enterprise Architecture**
  - DoDAF/MODAF architecture frameworks
  - Languages for interoperability
- **Military systems**
  - Both communications and C4I command/control
- **Civil Government**
  - Electronic records management
  - Skills management (Japanese-led)
- **Robotics, Healthcare, Manufacturing, etc.**

Government-Specific Focus

- **Engaged civil governments include U.S., Japan, Central America (led by Costa Rica), U.K.**
- **Primary focus areas**
  - Federal Enterprise Architecture Transition Framework
  - Records Management Services
  - Skills Management & Modeling
  - Performance-based Acquisition Modeling

Military Communications

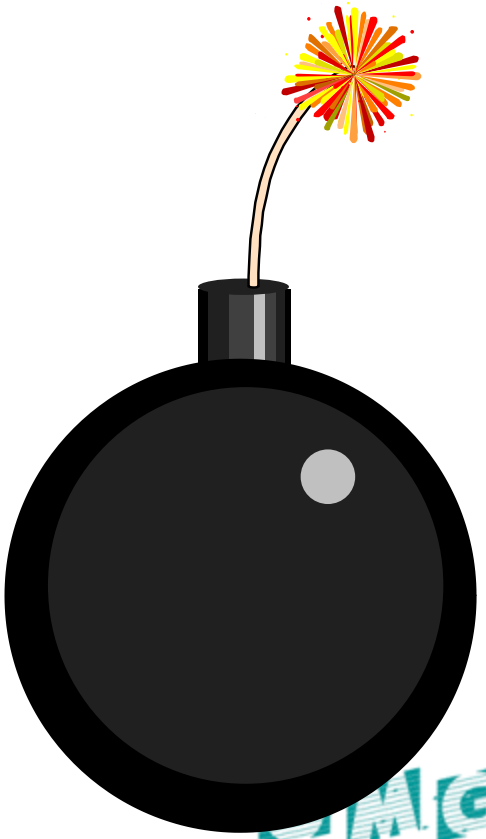
- **Focus of the Software Based Communications Domain Task Force is actually general**
  - Multi-frequency, multi-protocol radio communciation
  - Software-based for agility
  - JTRS Software Communications Architecture
  - Strong joint development with Wireless Innovation Forum (WINF, née SDR Forum)
  - Long-term cooperation with JTRS JPEO

Command & Control

- **Strong participation especially from U.S., U.K., Canada (joint leadership)**
- **Other participation includes NATO, Australia, Japan, etc.**
- **Focused on information integration from the small (sonar grids) to the large (SOPES, Shared Operational Picture Exchange Services)**
- **Application to emergency response also**

Software Quality: An Example

- **Regardless of methodology & approach, the biggest problem in IT today is inconsistent and unreliable software quality**
- **This is another major OMG focus**



The Software Quality Dilemma

National Research Council
Software for Dependable Systems


review articles

Who could fault an approach that offers greater credibility at reduced cost?

BY DANIEL JACKSON

A Direct Path to Dependable Software

SOFTWARE PLAYS A fundamental role in our society, bringing enormous benefits to all fields. But because many of our current systems are highly centralized and tightly coupled,[1] we are also susceptible to massive and coordinated failure.

A Chicago hospital lost its entire pharmacy database one night, and it was only able to reconstruct medication records for its patients by collecting paper printouts from nurses' stations. In their report on this incident,[2] Richard Cook and Michael O'Connor concluded: "Accidents are signals sent from deep within the system about the sorts of vulnerability and potential for disaster that lie within." Similar signals have been sent, for example, in the fields of electronic voting,[3] air traffic control,[4] nuclear power,[5] and energy distribution.[6]

The growing tendency to embed

"As higher levels of assurance are demanded…testing cannot deliver the level of confidence required at a reasonable cost."

"The cost of preventing all failures will usually be prohibitively expensive, so a dependable system will not offer uniform levels of confidence across all functions."

"The correctness of the code is rarely the weakest link."

Jackson, D. (2009). Communications of the ACM, 52 (4)

Software Engineering's 4th Wave

What: Architecture, Quality characteristics, Reuse
When: 2002➔
Why: Ensure software is constructed to standards that meet the lifetime demands placed on it

What: CMM/CMMI, ITIL, PMBOK, Agile
When: 1990-2002
Why: Provide a more disciplined environment for professional work incorporating best practices

What: Design methods, CASE tools
When: 1980-1990
Why: Give developers better tools and aids for constructing software systems

What: 3rd & 4th generation languages, structured programming
When: 1965-1980
Why: Give developers greater power for expressing their programs

Why CISQ?

- **Industry needs software quality measures:**
  - Visibility into business critical applications
  - Control of outsourced work
  - Benchmarks

- **Current limitations:**
  - Manual, expensive➔infrequent use
  - Subjective➔not repeatable or comparable
  - Inconsistent definitions➔burdens usage

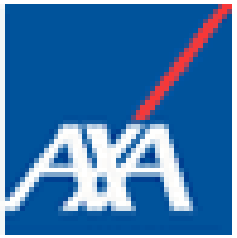
What Is CISQ?

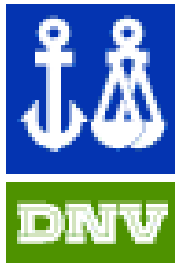
Carnegie Mellon
Software Engineering Institute

OBJECT MANAGEMENT GROUP

OBJECT MANAGEMENT GROUP

CISQ Members





Initial CISQ Objectives

1. Raise international awareness of the critical challenge of IT software quality
2. Develop standard, automatable measures and anti-patterns for evaluating IT software quality
3. Promote global acceptance of the standard in acquiring IT software and services
4. Develop an infrastructure of authorized assessors and products using the standard

CISQ Operations

- **CISQ Executive Meetings**
  - Annual Executive Forums
  - Quarterly Webinars on progress and special topics
- **Quarterly CISQ Technical Meetings**
  - Initiated Q1 2010
  - Virtual to the extent possible
  - Distributed work on prioritized quality attributes
- **Member Involvement**
  - Executives – 1 day per year
  - Delegates – 2-4 weeks per year

CISQ Deployment

Promote global acceptance of the standard in acquiring IT application software and services:

- ✓ Establish industry consensus on the use of an IT application quality standard as a component of the acceptance criteria for contracted/supplied software
- ✓ Develop guidance for incorporating IT application quality criteria in contractor/outsourcer/vendor contracts
- ✓ Collect information/data on the use of IT application quality criteria in contractor/outsourcer/vendor contracts to improve their definition and use

Future CISQ Directions

- **CISQ will pursue member-driven objectives**
  - Determined by CISQ Executive Forum
  - Consensus among CISQ members of problem to be addressed
- **Early requests for additional objectives:**
  - Defect and failure-related definitions
  - Business value measures related to application quality
  - Size measures
- **Use of Executive Forum for addressing industry issues**
  - Quality-based SLAs in outsourcing contracts
  - Benchmarking
  - Industry response to regulatory challenges

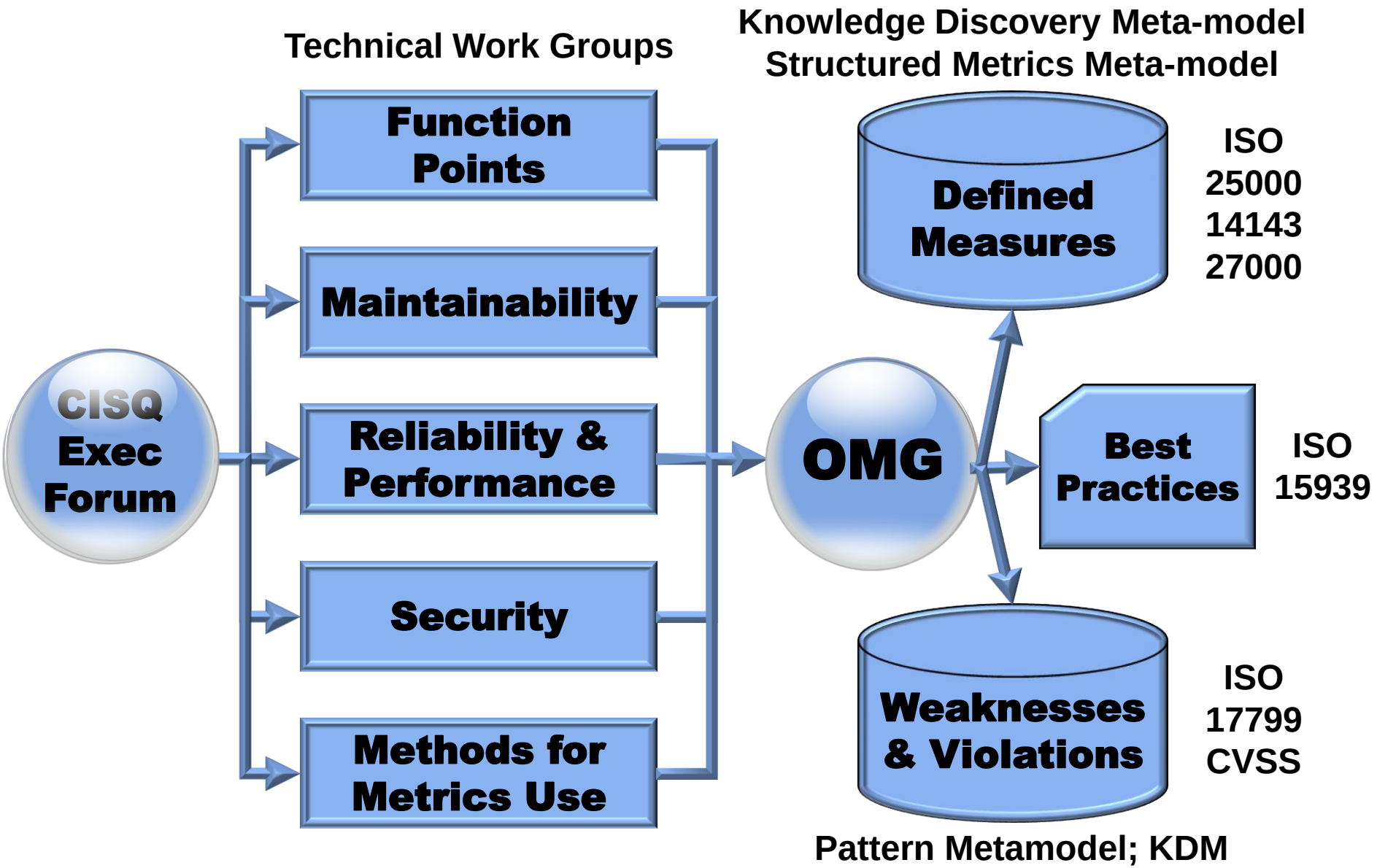
CISQ Vision

- **In 2011, there will be an open, neutral, objective standard for measuring the quality of software code based only on the code itself.**

- **In 2011, there will be a recognized, international, neutral authority that licenses individuals trained to apply the above standard in software quality analyses and provide related software quality services.**

- **In 2011, there will be an international market of software quality metrics products supporting the standard widely available from multiple vendors.**

CISQ Standards Process



CISQ Standards

The CISQ project is developing an OMG standard defining computable measures and anti-patterns to be used for evaluating multi-tier IT application software:

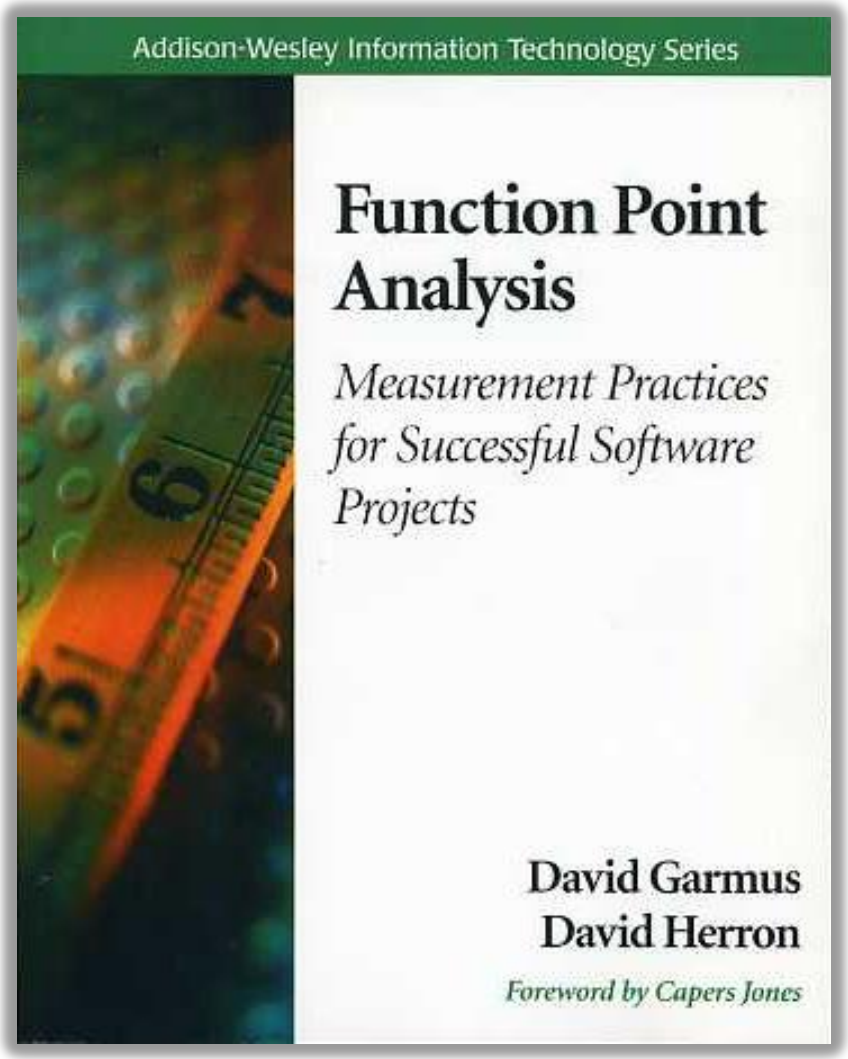
- ✓ Establish a computable software quality standard for IT applications with scoring guidelines
- ✓ Recommend measurement thresholds against which minimally acceptable levels of quality and other attributes of business application software can be assessed.
- ✓ Develop baselines for benchmarking application quality, productivity, cost, and other attributes across application domains and industry segments.
- ✓ Conduct case study research with consortium sponsors validating application metrics and their business value.
- ✓ Provide a source of application measurement expertise to consortium sponsors.

OBJECT MANAGEMENT GROUP

Size Technical Work Group

Objective

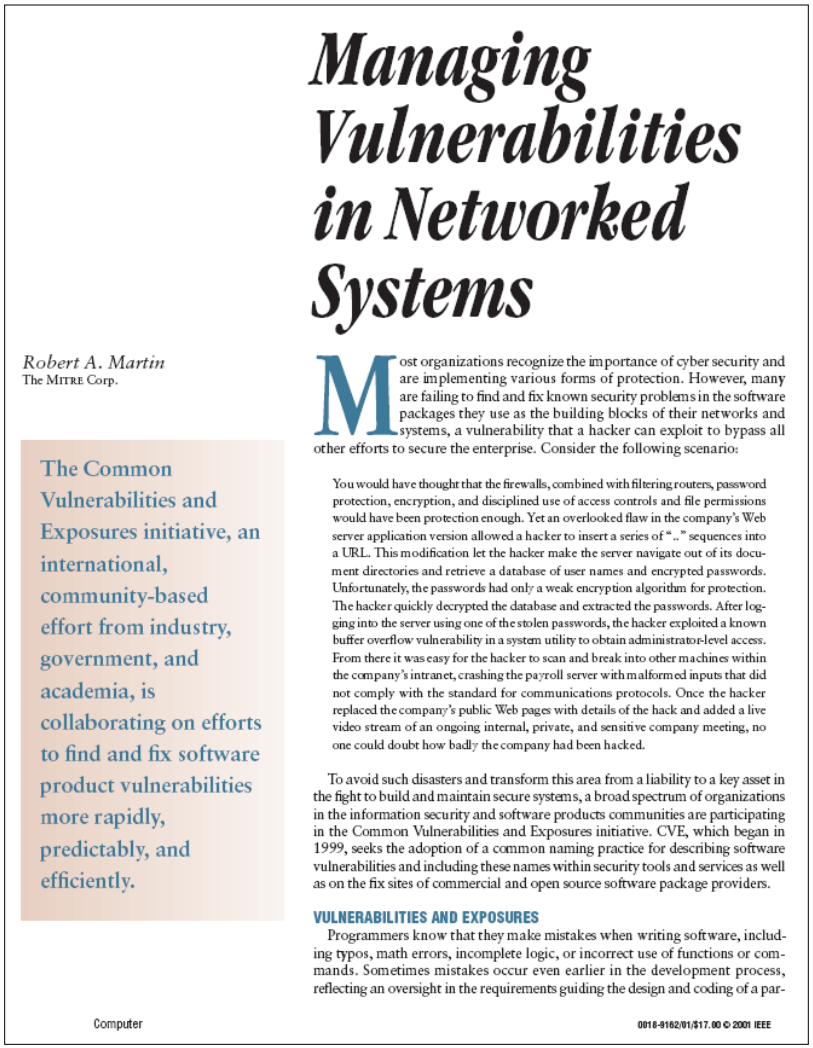
Create a definition of Function Points that is as close to IFPUG counting rules as possible, while resolving the issues necessary to enable fully automated counting at the source code level



Security Technical Work Group

Objective

Develop automated source code measures that predict the vulnerability of source code to external attack. Coordinate work products with work in the software assurance community



Managing Vulnerabilities in Networked Systems

Robert A. Martin
The MITRE Corp.

The Common Vulnerabilities and Exposures initiative, an international, community-based effort from industry, government, and academia, is collaborating on efforts to find and fix software product vulnerabilities more rapidly, predictably, and efficiently.

Most organizations recognize the importance of cyber security and are implementing various forms of protection. However, many are failing to find and fix known security problems in the software packages they use as the building blocks of their networks and systems, a vulnerability that a hacker can exploit to bypass all other efforts to secure the enterprise. Consider the following scenario:

> You would have thought that the firewalls, combined with filtering routers, password protection, encryption, and disciplined use of access controls and file permissions would have been protection enough. Yet an overlooked flaw in the company's Web server application version allowed a hacker to insert a series of "../" sequences into a URL. This modification let the hacker make the server navigate out of its document directories and retrieve a database of user names and encrypted passwords. Unfortunately, the passwords had only a weak encryption algorithm for protection. The hacker quickly decrypted the database and extracted the passwords. After logging into the server using one of the stolen passwords, the hacker exploited a known buffer overflow vulnerability in a system utility to obtain administrator-level access. From there it was easy for the hacker to scan and break into other machines within the company's intranet, crashing the payroll server with malformed inputs that did not comply with the standard for communications protocols. Once the hacker replaced the company's public Web pages with details of the hack and added a live video stream of an ongoing internal, private, and sensitive company meeting, no one could doubt how badly the company had been hacked.

To avoid such disasters and transform this area from a liability to a key asset in the fight to build and maintain secure systems, a broad spectrum of organizations in the information security and software products communities are participating in the Common Vulnerabilities and Exposures initiative. CVE, which began in 1999, seeks the adoption of a common naming practice for describing software vulnerabilities and including these names within security tools and services as well as on the fix sites of commercial and open source software package providers.

VULNERABILITIES AND EXPOSURES

Programmers know that they make mistakes when writing software, including typos, math errors, incomplete logic, or incorrect use of functions or commands. Sometimes mistakes occur even earlier in the development process, reflecting an oversight in the requirements guiding the design and coding of a par-

0018-9162/01/$17.00 © 2001 IEEE

OMG
OBJECT MANAGEMENT GROUP

CISQ Status

- **Executive Forums in Frankfurt, Germany; Washington, USA & Bangalore, India**
- **Five Technical Work Groups established**
  - **Based on Executive Forum priorities**
  - **Member assignment of delegates underway**
- **Standards targeted for 2011, first draft for some Work Groups expected in December 2010**

Value of Membership

- **Direct Access to Industry Leading Subject Matter Experts**
- **Access to the knowledge Best Practices from Multiple Operational and Technology Domains**
- **Influence Direction of Next Generation Products**
- **Ensure your requirements are known**

Value of Participation

- **Know the direction of standards *before* public adoption begins: be a market leader**
- **Influence the direction of standards: leadership saves time & money downstream**
- **Access to documents, presentations, white papers, design decisions before public access and completion**
- **Gain recognition for leadership by speaking, publishing & *leading***

To Get More Information

- **OMG General Information**
  - http://www.omg.org/
- **Business Ecology Initiative**
  - http://www.business-ecology.org/
- **IT Software Quality Initiative**
  - http://it-cisq.org/
- **Contact the Author**
  - soley@omg.org