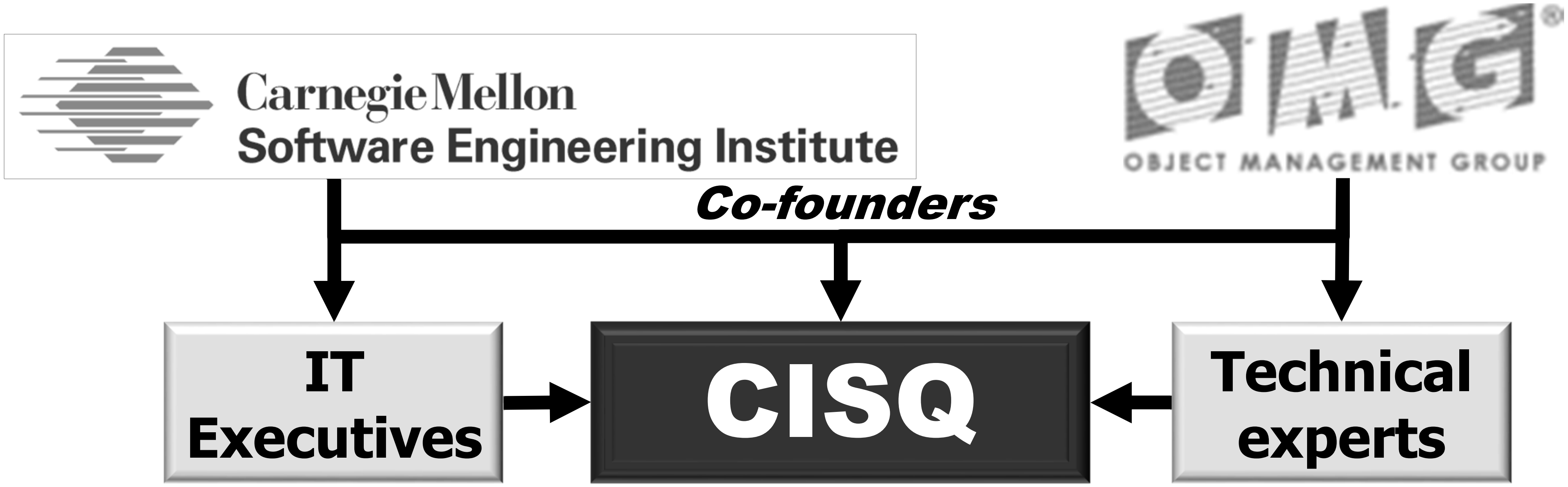
CONSORTIUM FOR IT SOFTWARE QUALITY

New Standards for Automating Source Code Analysis of Structural Quality

Dr. Bill Curtis

Executive Director, CISQ

CISQ Founders and Sponsors



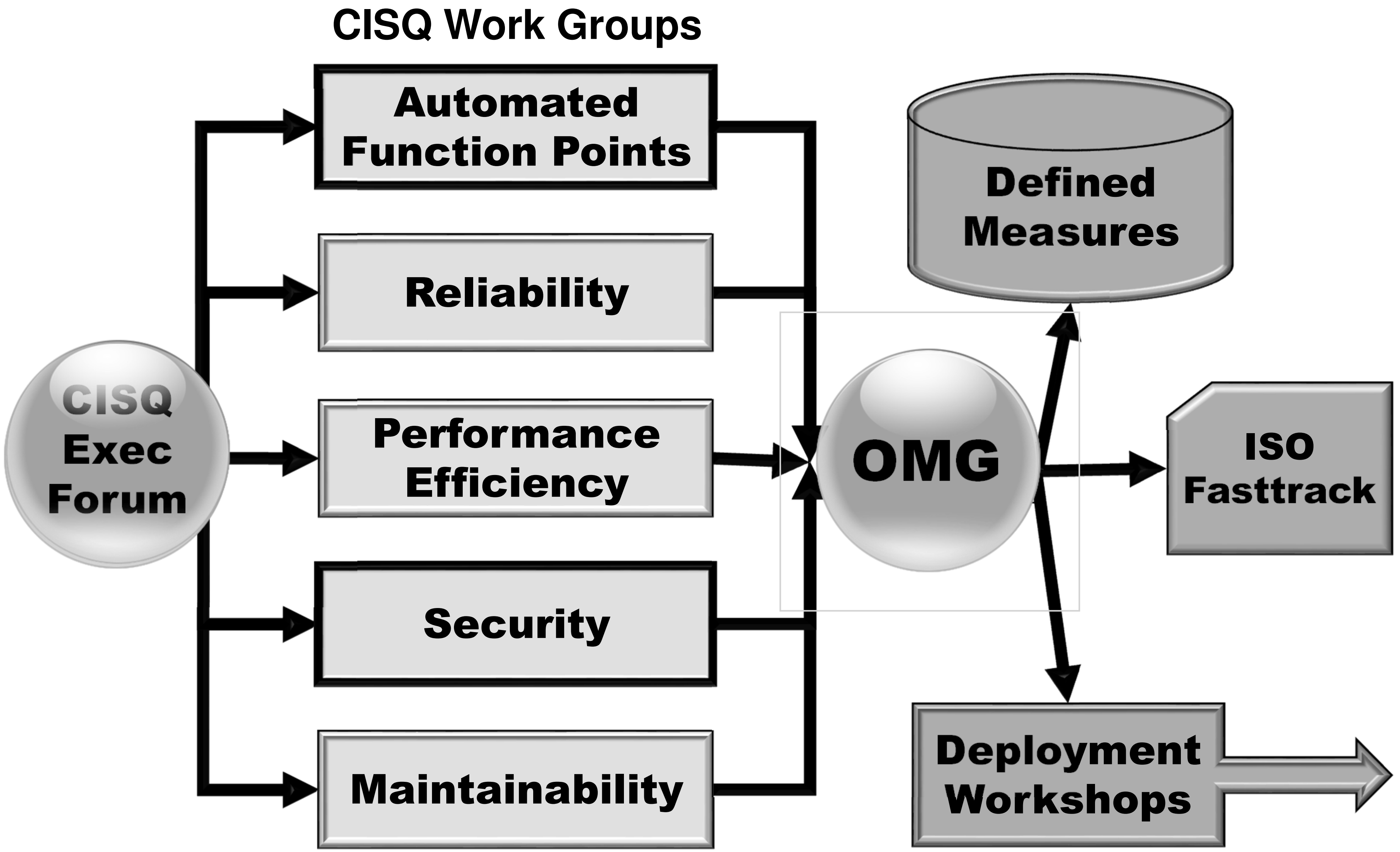
OMG Special Interest Group

Develop standard, automatable measures for evaluating software size and quality with an ecosystem supporting policy and deployment

CISQ Sponsors

CISQ

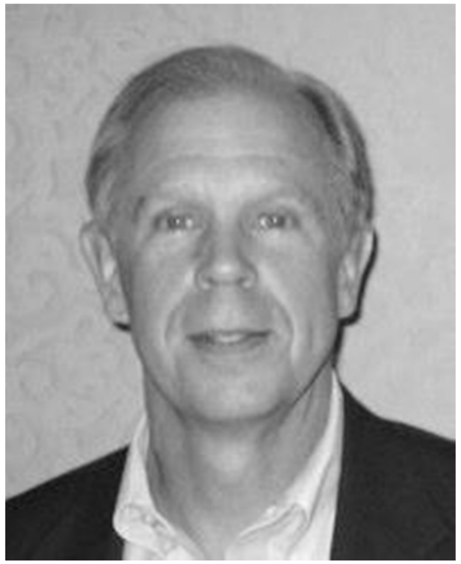
CISQ/OMG Standards Process

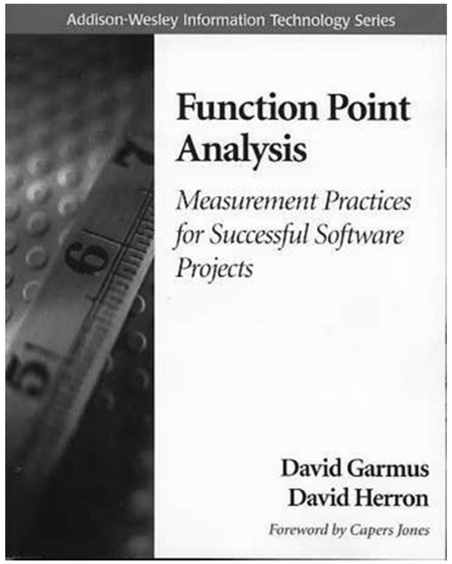


CISQ

Automated FP Specification

- **OMG Supported Specification for Automated Function Points**
- **Mirrors IFPUG counting guidelines, but automatable**
- **Specification developed by international team led by David Herron of David Consulting Group**



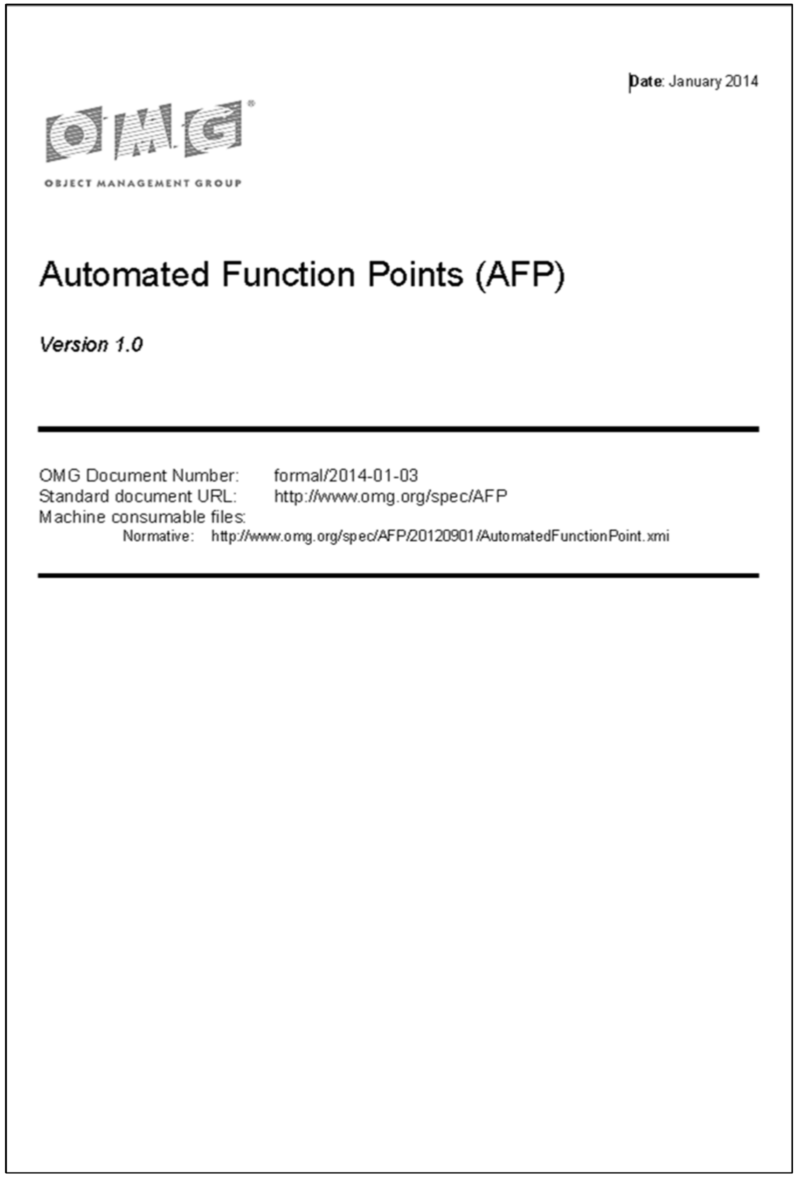

Addison-Wesley Information Technology Series

Function Point Analysis

Measurement Practices for Successful Software Projects

David Garmus
David Herron

Foreword by Capers Jones


Date: January 2014

OMG
OBJECT MANAGEMENT GROUP

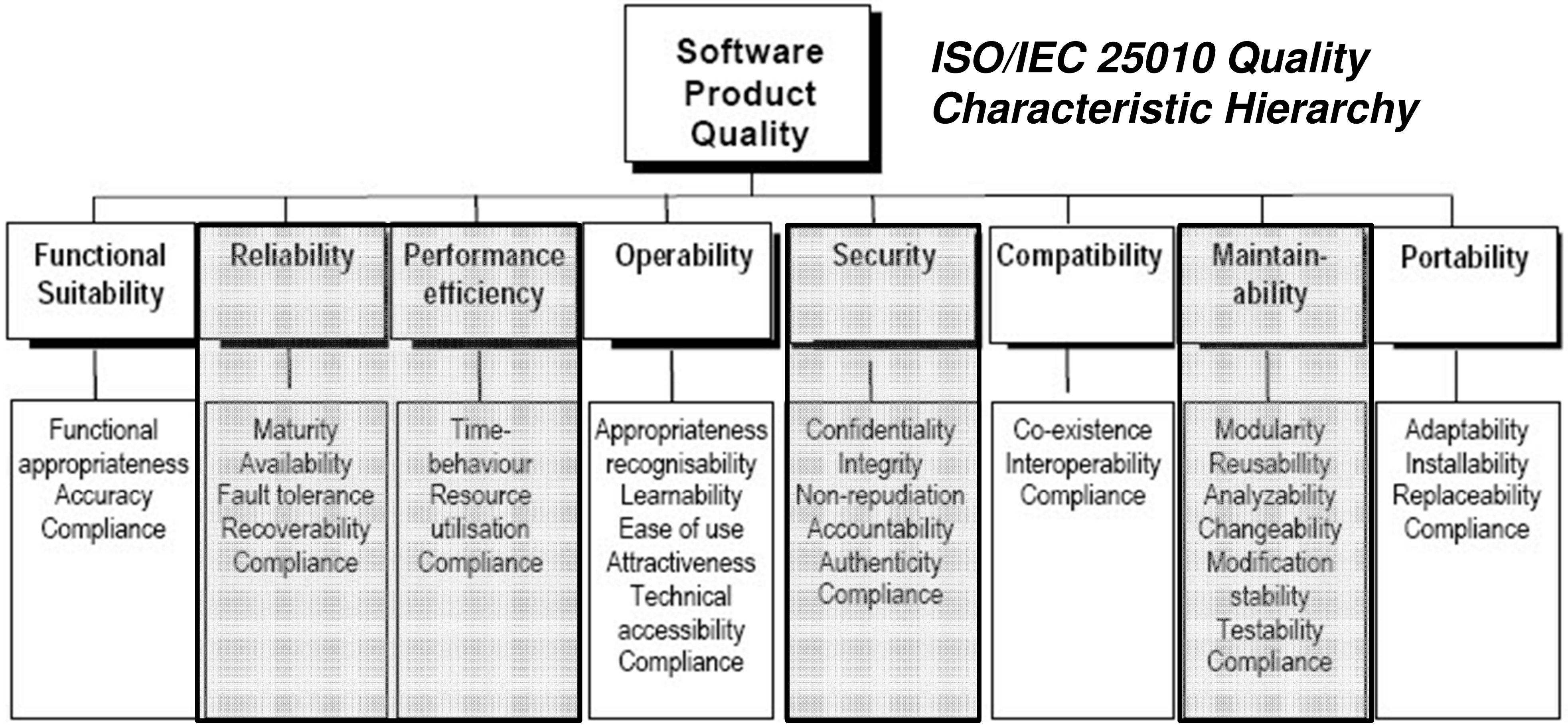
Automated Function Points (AFP)

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

CISQ Measures and ISO 25010

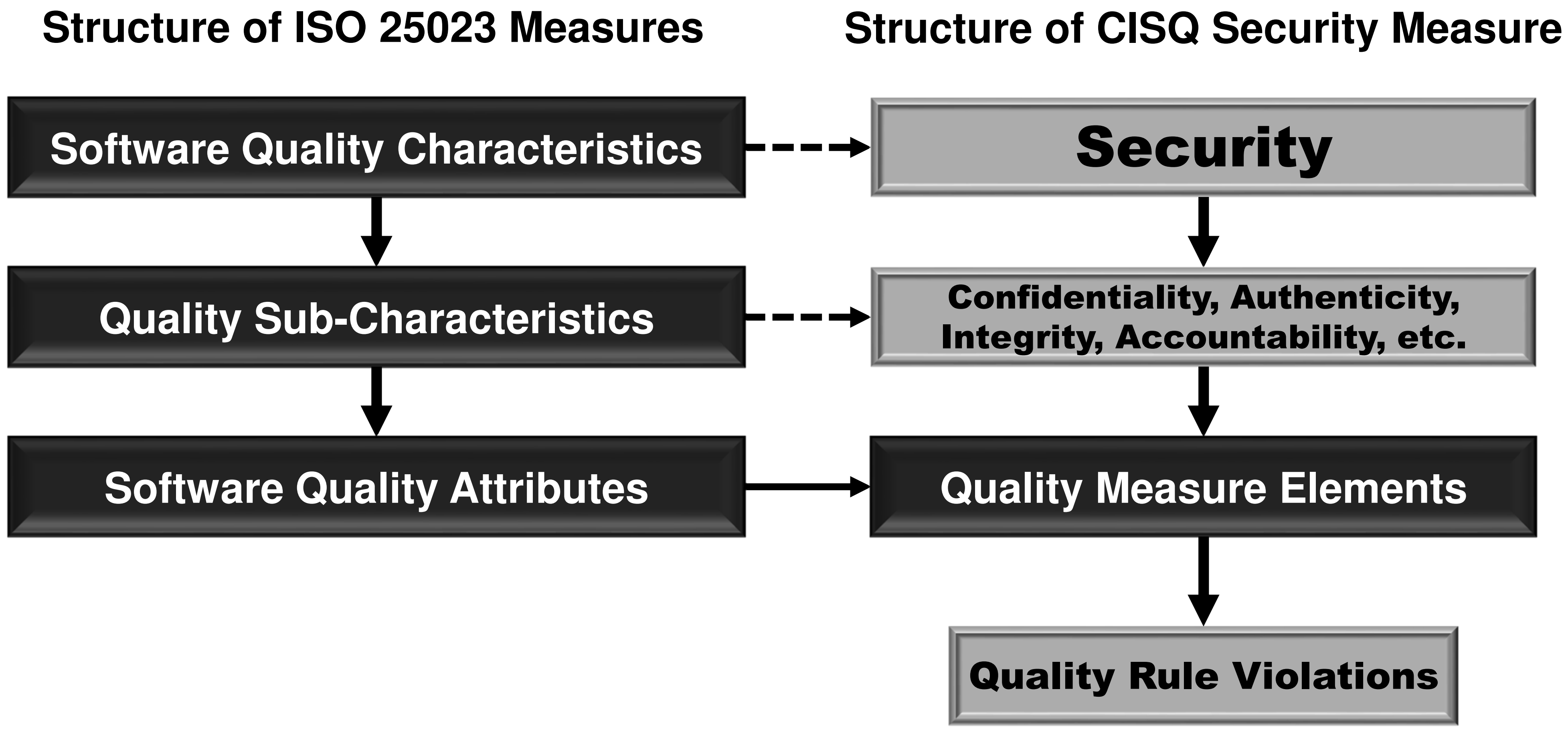
- ISO 25010 defines quality characteristics and sub-characteristics
- ISO 25023 defines measure elements for each sub-characteristic
- ISO 25023 does not define measures at the source code level
- CISQ supplements ISO 25023 by defining code level measures


Software Product Quality
Functional Suitability
Reliability
Performance efficiency
Operability
Security
Compatibility
Maintain-ability
Portability
Functional appropriateness Accuracy Compliance
Maturity Availability Fault tolerance Recoverability Compliance
Time-behaviour Resource utilisation Compliance
Appropriateness recognisability Learnability Ease of use Attractiveness Technical accessibility Compliance
Confidentiality Integrity Non-repudiation Accountability Authenticity Compliance
Co-existence Interoperability Compliance
Modularity Reusabillity Analyzability Changeability Modification stability Testability Compliance
Adaptability Installability Replaceability Compliance

ISO/IEC 25010 Quality Characteristic Hierarchy

CISQ defining automatable measures for characteristics highlighted in orange

CISQ Quality Measure Structure



Structure of ISO 25023 Measures
Structure of CISQ Security Measure
Software Quality Characteristics
Security
Quality Sub-Characteristics
Confidentiality, Authenticity, Integrity, Accountability, etc.
Software Quality Attributes
Quality Measure Elements
Quality Rule Violations

■ ISO structure

▨ Examples from CISQ measures

- Cross-site scripting
- SQL injection
- Buffer overflow
- OS command injection
- Unvalidated array
- Etc.

CISQ CWEs in CISQ Security Measure

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')

CWE

Common Weakness Enumeration

Robert Martin
MITRE

Focus Shift in Diagnostic Metrics

Traditional metrics — measure program elements such as tokens, objects, or control structures

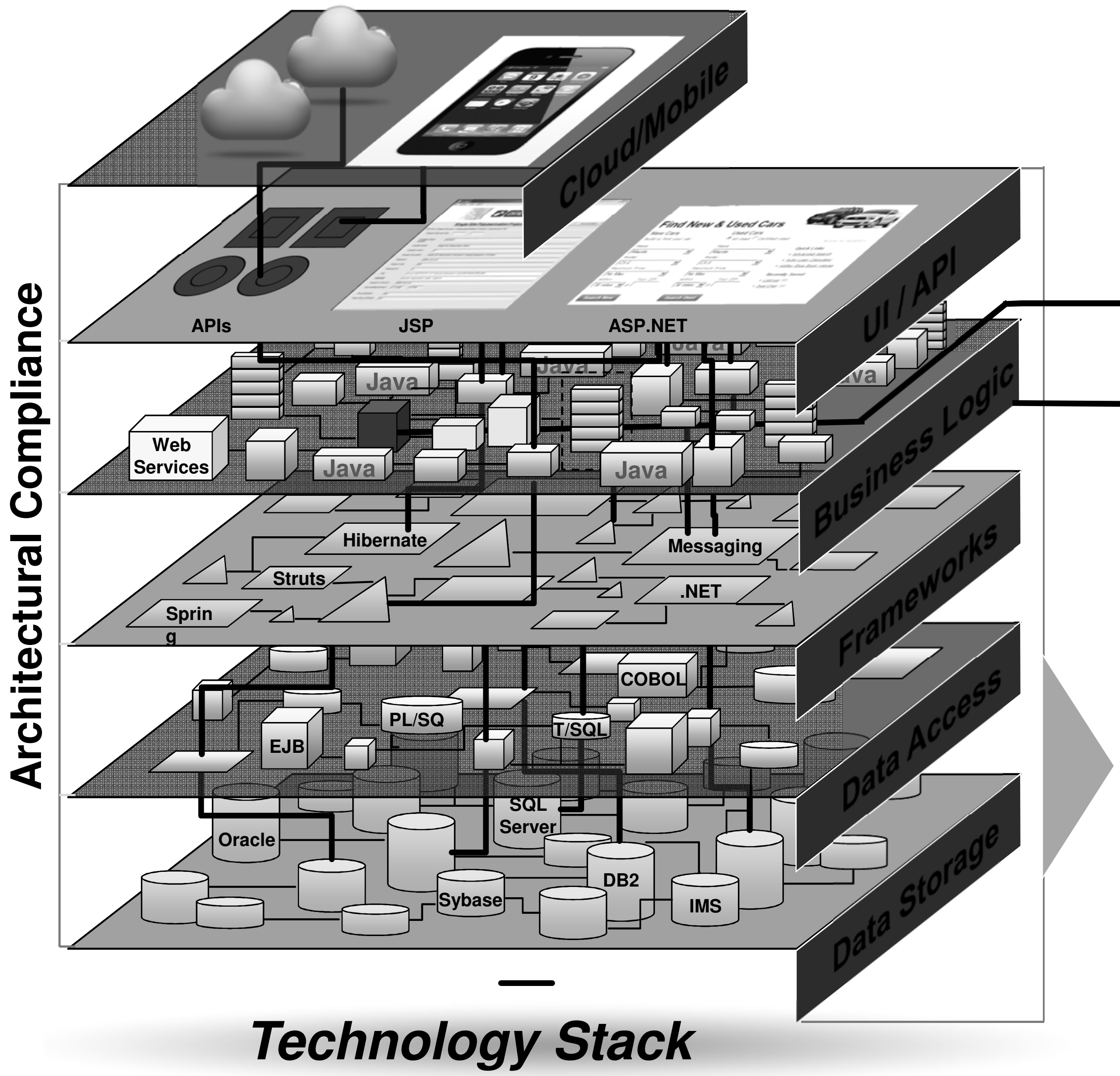
These elements correlate with the potential for defects

These elements are defects

Violation metrics — measure violations of good architectural and coding practice

Violations can be analyzed as patterns

CISQ IT Quality Challenge — System Level



1 Unit Level

- Code style & layout
- Expression complexity
- Code documentation
- Class or program design
- Basic coding standards
- Developer level

2 Technology Level

- Single language/technology layer
- Intra-technology architecture
- Intra-layer dependencies
- Inter-program invocation
- Security vulnerabilities
- Development team level

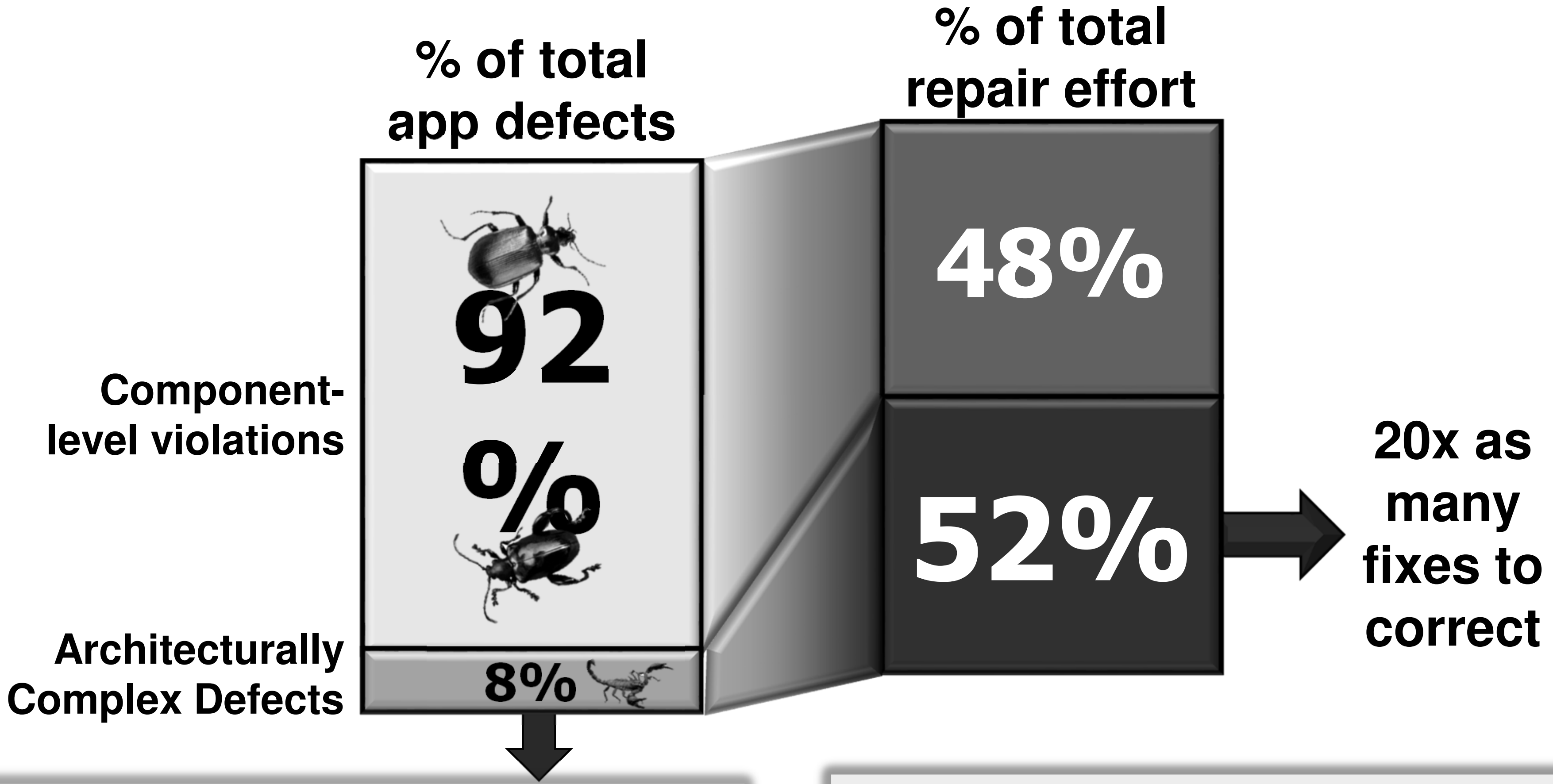
3 System Level

- Integration quality
- Architectural compliance
- Risk propagation
- Application security
- Resiliency checks
- Transaction integrity
- Function point,
- Effort estimation
- Data access control
- SDK versioning
- Calibration across technologies
- IT organization level

CISQ

Architecturally Complex Defects

Architecturally Complex Defect	A structural flaw involving interactions among multiple components that reside in different application layers

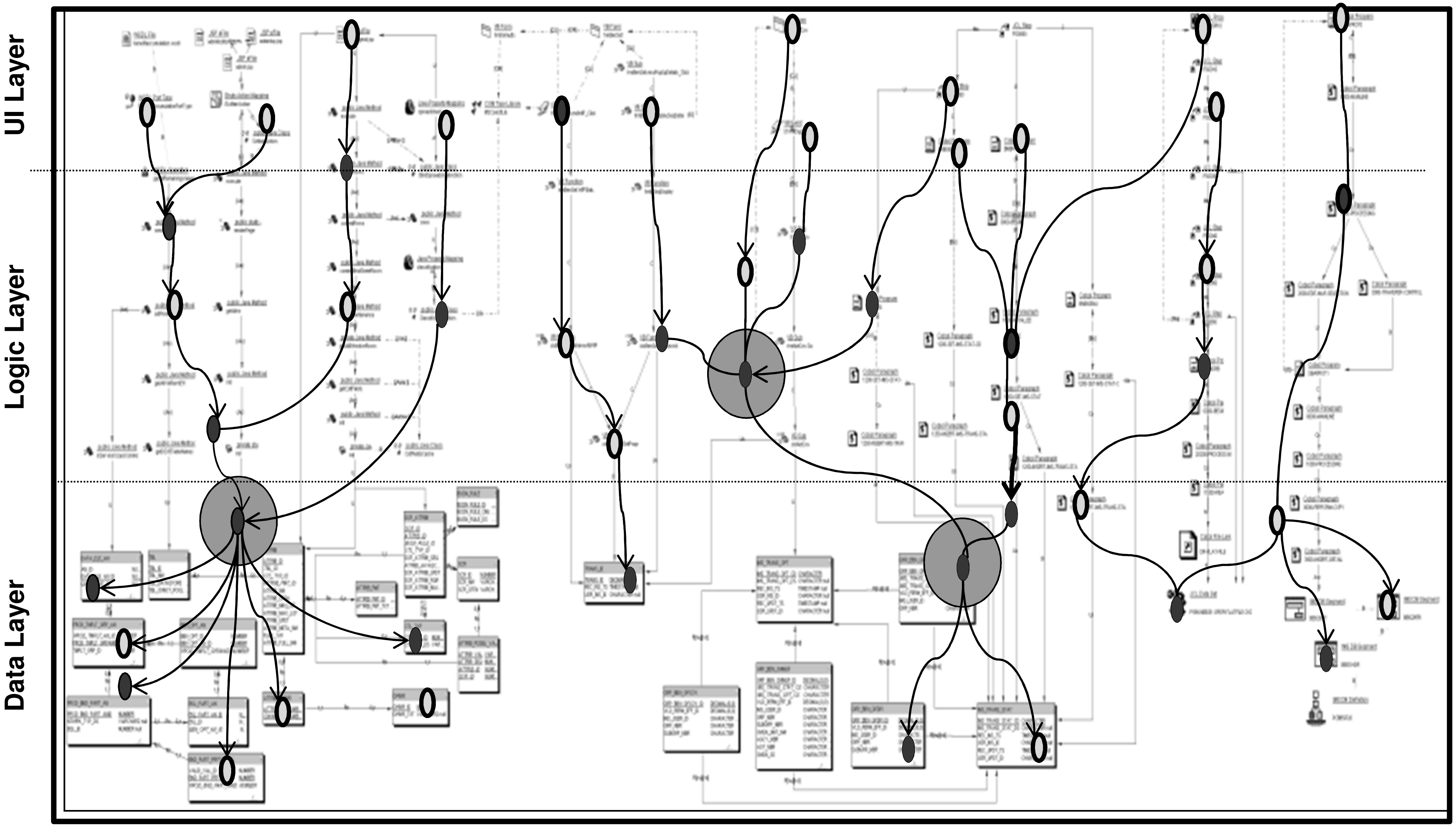


80% of architecturally complex defects touch an Architectural Hotspot—a badly designed component causing problems

Architectural hotspots provide a roadmap for remediating the worst risk, rework, and cost drivers

CISQ

Detecting Architectural Hotspots



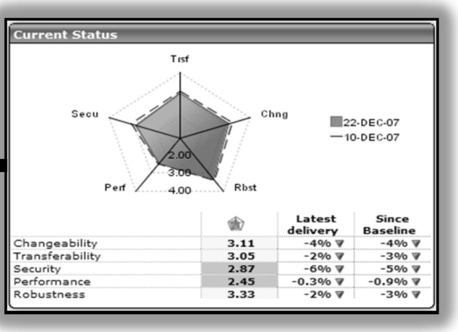
⬬ **Contributor to architecturally complex defect**

⬬ **Architectural hotspot**

CISQ

Structural Quality Measure Uses

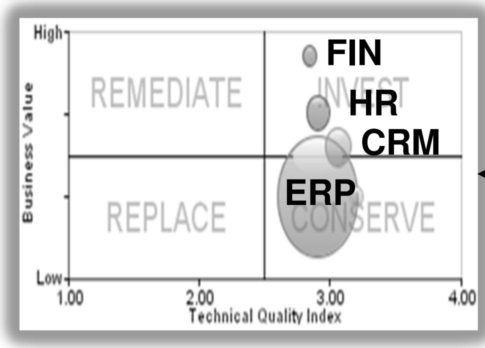
Acquisition Managers


Current Status

		Latest delivery	Since Baseline
Changeability	3.11	-4% ▼	-4% ▼
Transferability	3.05	-2% ▼	-3% ▼
Security	2.87	-6% ▼	-5% ▼
Performance	2.45	-0.3% ▼	-0.9% ▼
Robustness	3.33	-2% ▼	-3% ▼

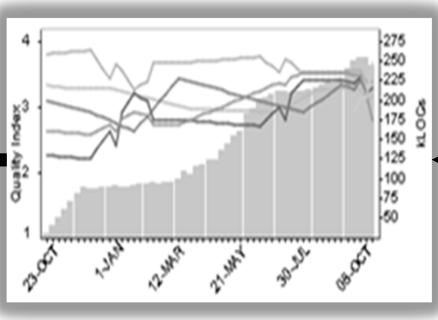
Deliverables insight

IT Executives



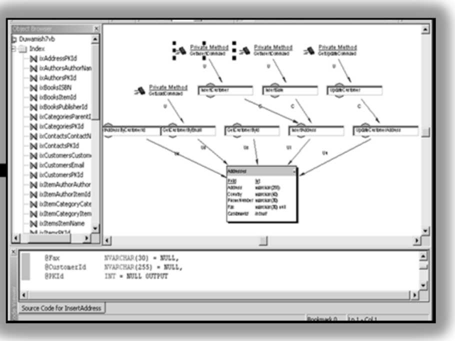
Portfolio insight

App / Project Managers



Application insight

Developers



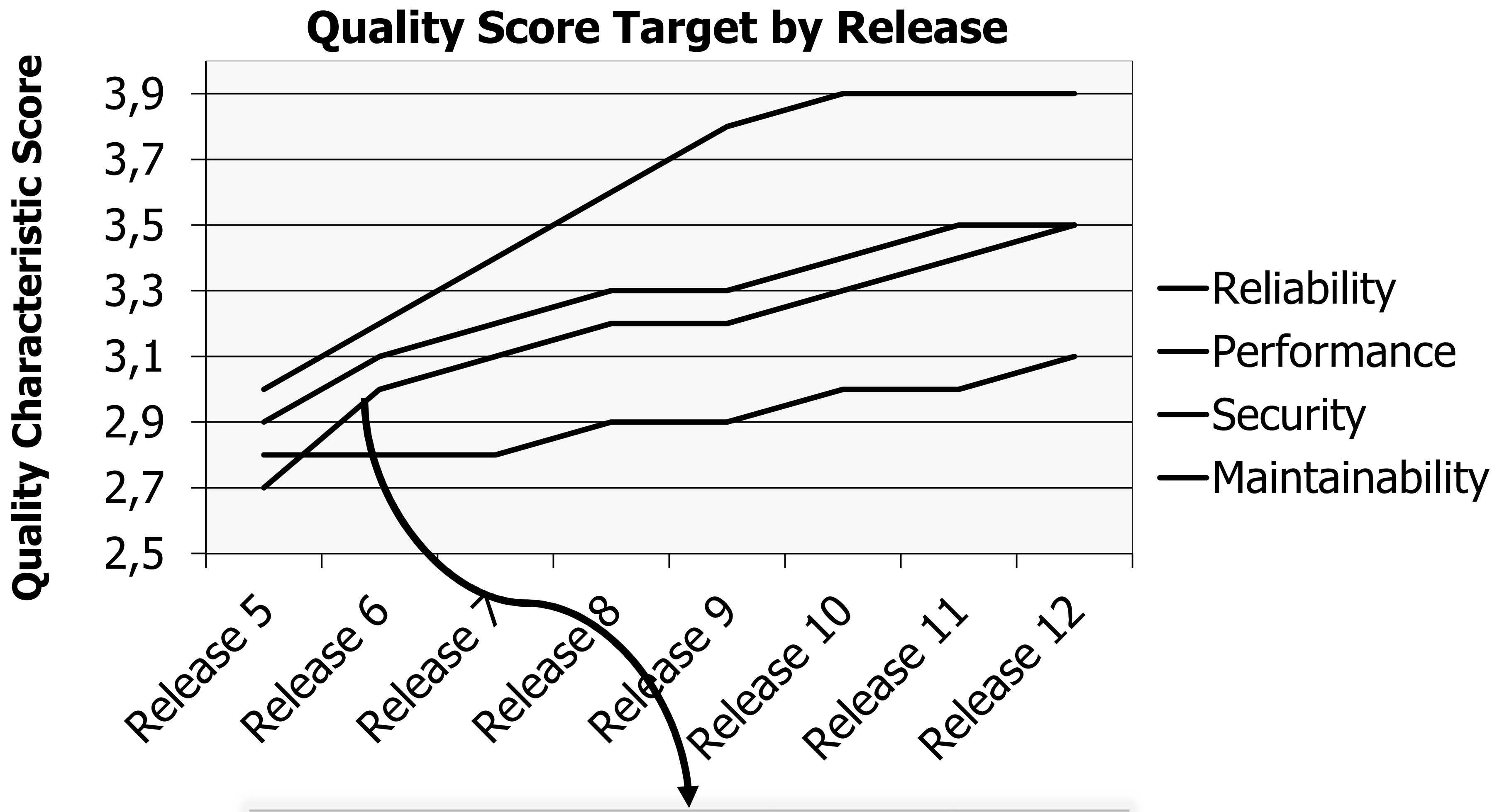
Remedial insight

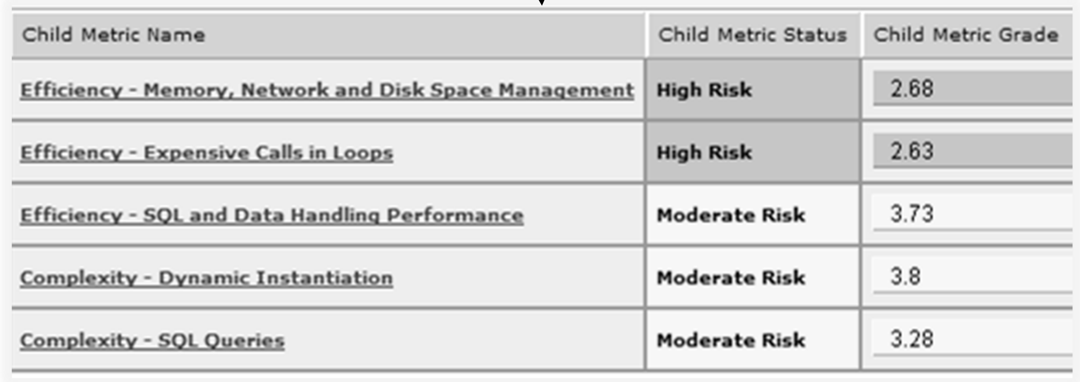
Using CISQ Measures with Vendors

1. Set compliance targets
2. FEnforce a measurement process
3. Evaluate contract deliverables
4. Use rewards and penalties wisely

CISQ

1 — Set Quality Compliance Targets

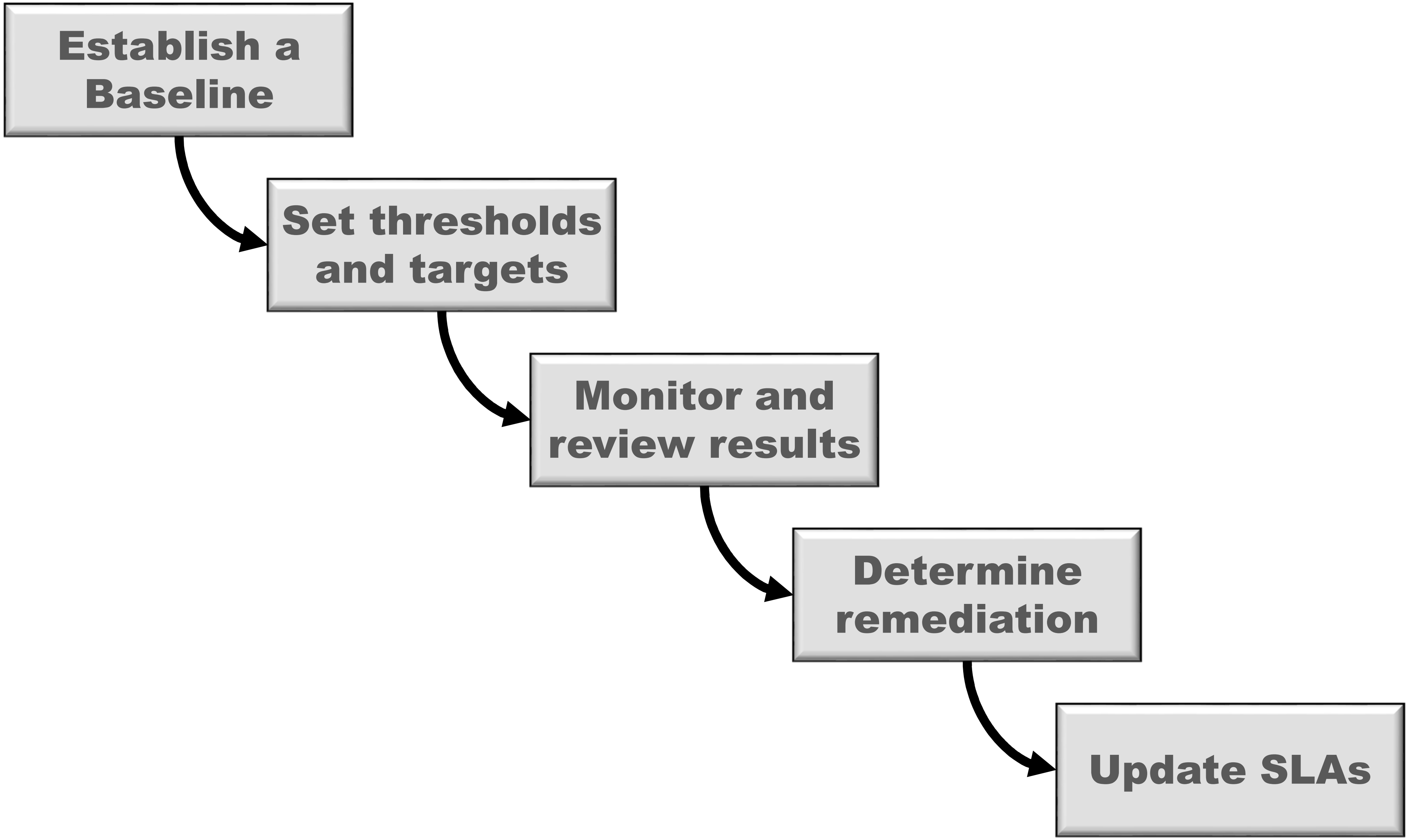




Child Metric Name	Child Metric Status	Child Metric Grade
Efficiency - Memory, Network and Disk Space Management	High Risk	2.68
Efficiency - Expensive Calls in Loops	High Risk	2.63
Efficiency - SQL and Data Handling Performance	Moderate Risk	3.73
Complexity - Dynamic Instantiation	Moderate Risk	3.8
Complexity - SQL Queries	Moderate Risk	3.28

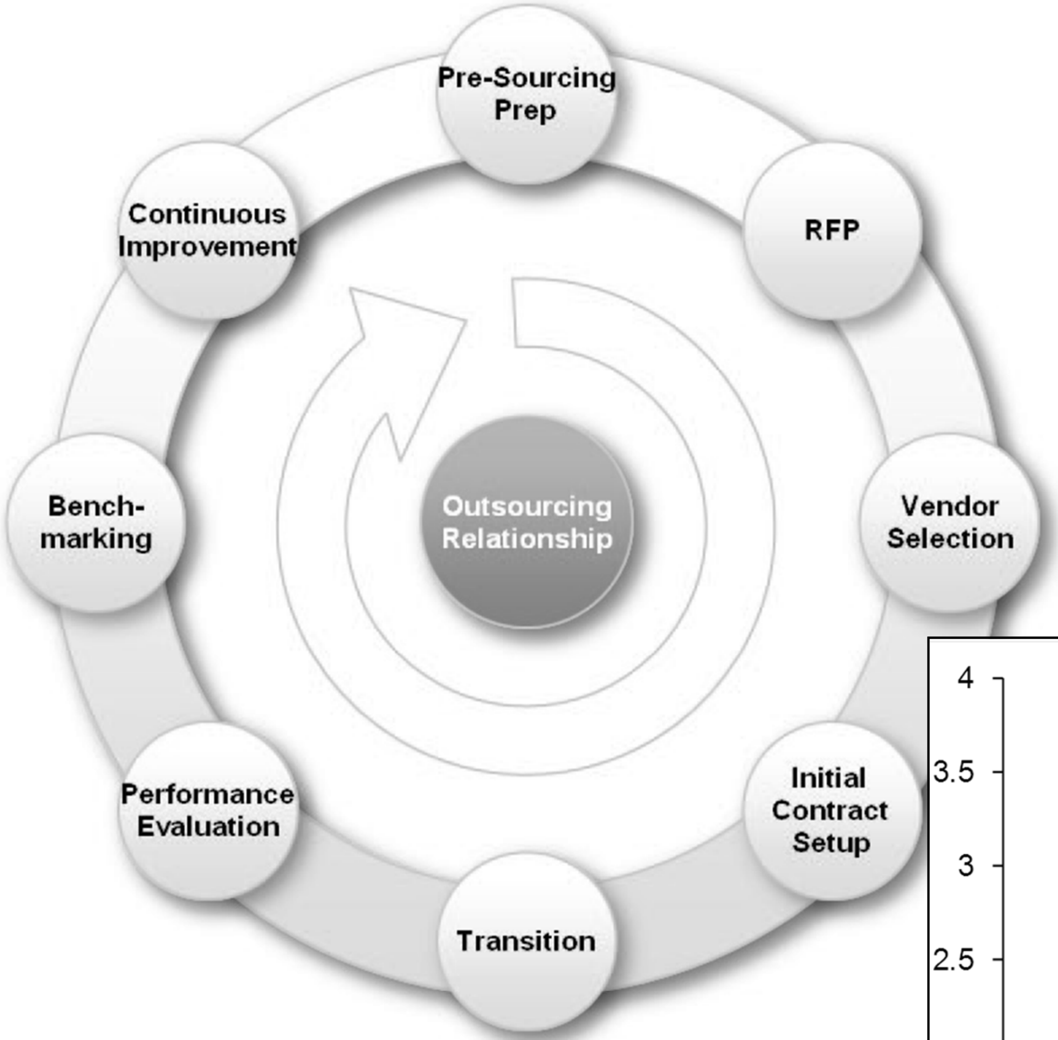
CISQ

2 — Enforce a Measurement Process

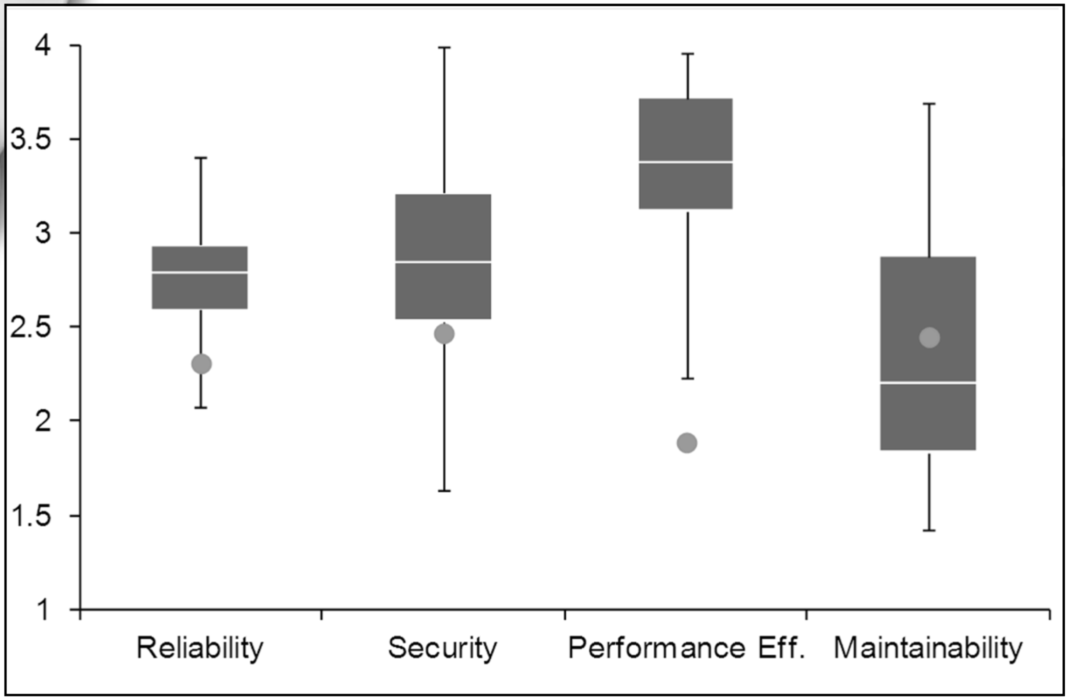


CISQ

3 — Evaluate Contract Deliverables



Use CISQ measures in contracts to establish objective, measureable agreements on quality priorities that comply with industry standards

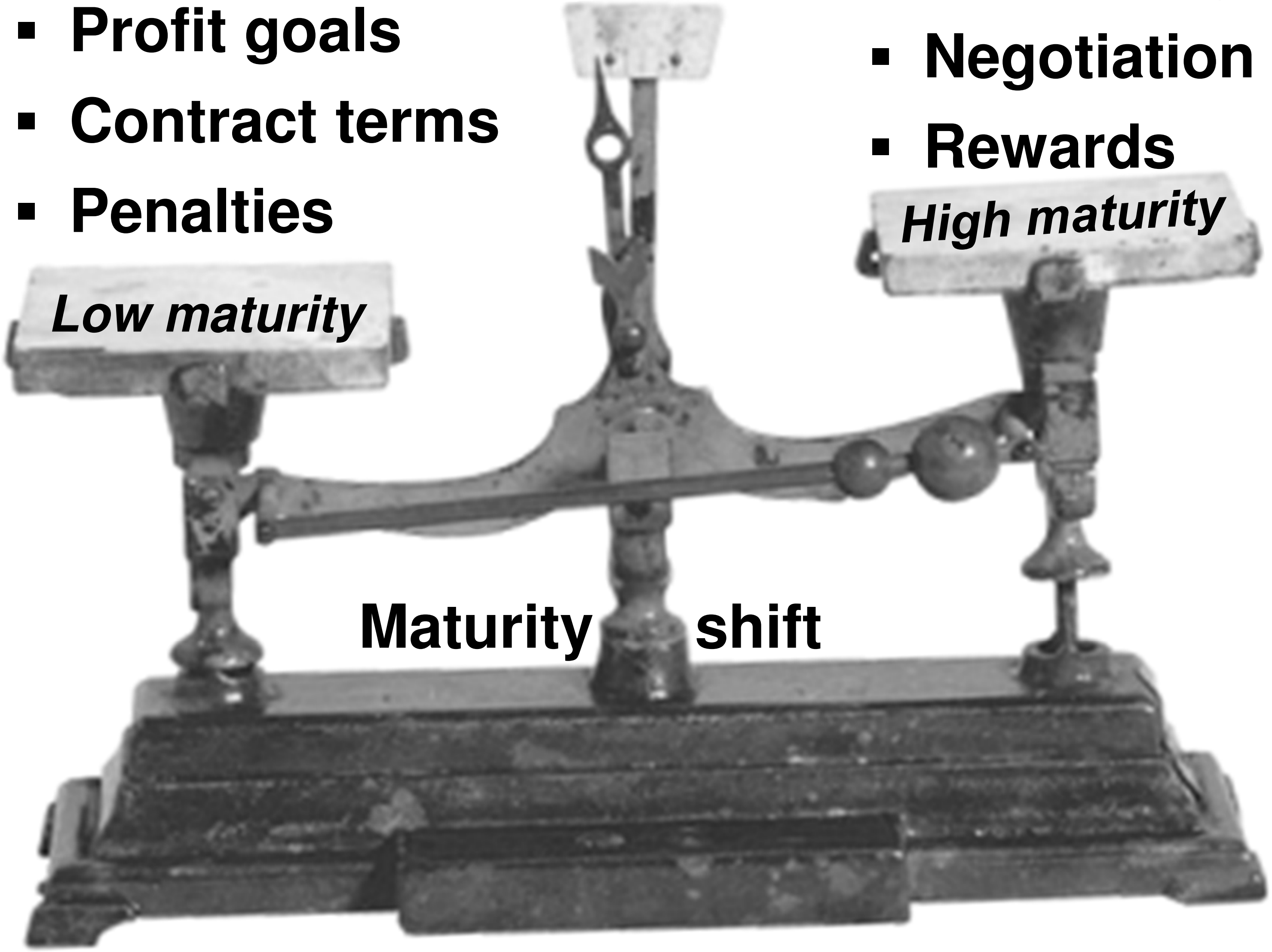


CISQ

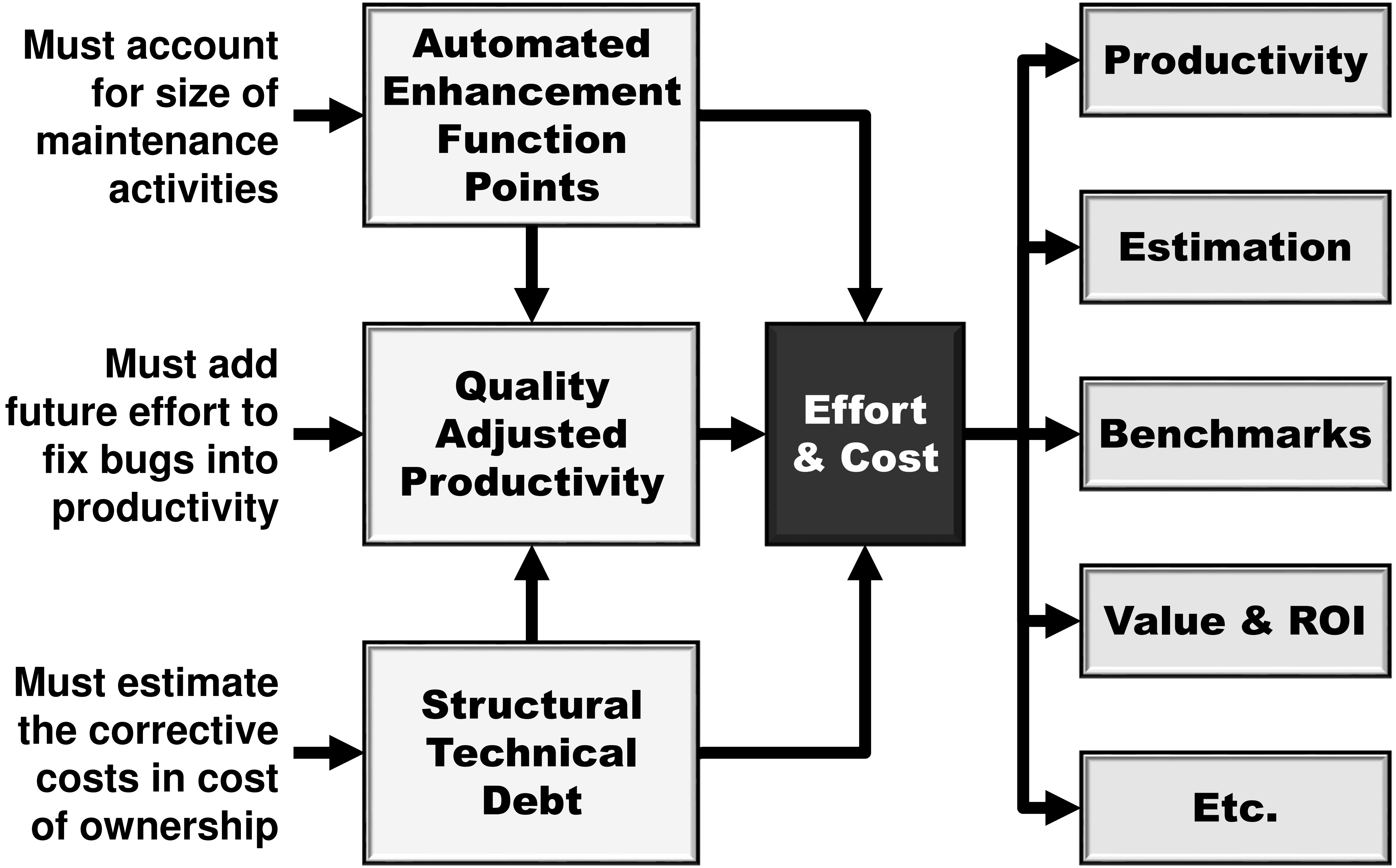
4 — Use Rewards and Penalties Wisely

- Vendor
- Profit goals
- Contract terms
- Penalties

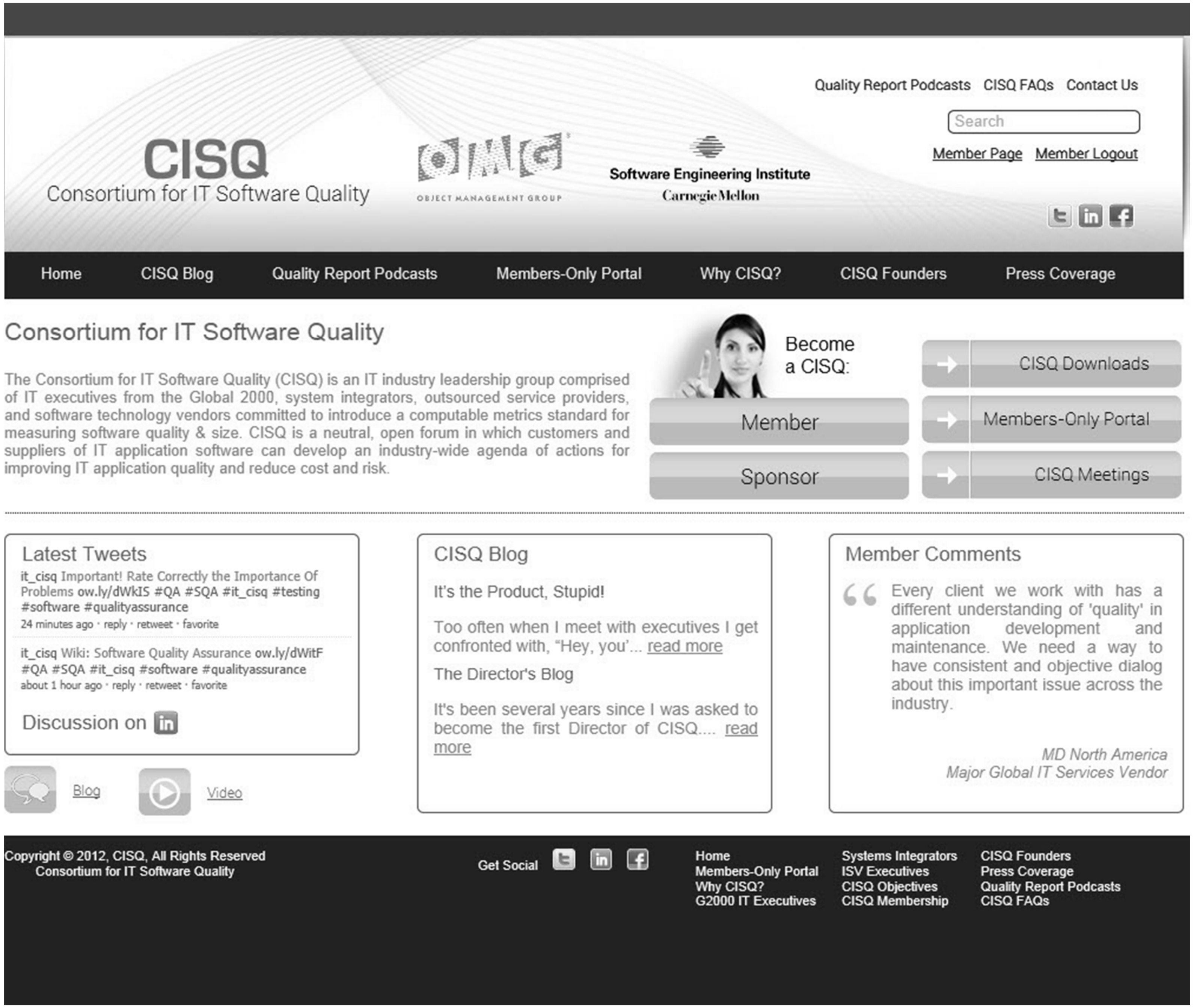
- Partnership
- Common goals
- Negotiation
- Rewards



CISQ New CISQ Measurement Specifications


Must account for size of maintenance activities
Automated Enhancement Function Points
Must add future effort to fix bugs into productivity
Quality Adjusted Productivity
Must estimate the corrective costs in cost of ownership
Structural Technical Debt
Effort & Cost
Productivity
Estimation
Benchmarks
Value & ROI
Etc.

CISQ **Join CISQ Free — www.it-cisq.org**


Quality Report Podcasts CISQ FAQs Contact Us

Search

Member Page Member Logout

CISQ
Consortium for IT Software Quality

OMG OBJECT MANAGEMENT GROUP

Software Engineering Institute
Carnegie Mellon

Home | CISQ Blog | Quality Report Podcasts | Members-Only Portal | Why CISQ? | CISQ Founders | Press Coverage

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 introduce 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 and reduce cost and risk.

Become a CISQ:

Member

Sponsor

CISQ Downloads

Members-Only Portal

CISQ Meetings

Latest Tweets

it_cisq Important! Rate Correctly the Importance Of Problems ow.ly/dWkIS #QA #SQA #it_cisq #testing #software #qualityassurance
24 minutes ago · reply · retweet · favorite

it_cisq Wiki: Software Quality Assurance ow.ly/dWitF #QA #SQA #it_cisq #software #qualityassurance
about 1 hour ago · reply · retweet · favorite

Discussion on in

Blog Video

CISQ Blog

It's the Product, Stupid!

Too often when I meet with executives I get confronted with, "Hey, you'... read more

The Director's Blog

It's been several years since I was asked to become the first Director of CISQ.... read more

Member Comments

"Every client we work with has a different understanding of 'quality' in application development and maintenance. We need a way to have consistent and objective dialog about this important issue across the industry.

MD North America
Major Global IT Services Vendor

Copyright © 2012, CISQ, All Rights Reserved
Consortium for IT Software Quality

Get Social

Home
Members-Only Portal
Why CISQ?
G2000 IT Executives

Systems Integrators
ISV Executives
CISQ Objectives
CISQ Membership

CISQ Founders
Press Coverage
Quality Report Podcasts
CISQ FAQs