Software Quality and Security Measures

Dr. Bill Curtis

SVP & Chief Scientist, CAST

Director, CISQ

Application Software Quantified
appmarq

CAST

Components of Internal Quality Analysis

Analyzers

- Oracle PL/SQL
- Sybase T-SQL
- SQL Server T-SQL
- IBM SQL/PSM
- C, C++, C#
- Pro C
- Cobol
- CICS
- Visual Basic
- VB.Net
- ASP.Net
- Java, J2EE
- JSP
- XML
- HTML
- Javascript
- VBScript
- PHP
- PowerBuilder
- Oracle Forms
- PeopleSoft
- SAP ABAP, Netweaver
- Tibco
- Business Objects Universal Analyzer

Application Knowledge Base

Technical Metrics

Application Health

Immediate Impact	*On-going Impact*
Robustness	Transferability
Performance	Changeability
Security	

Application Size

Technical Size	Functional Weight

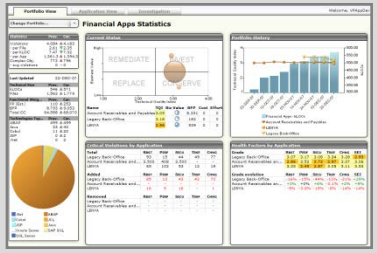
Application Metadata

Technical Inventory

Analysis of all system artifacts

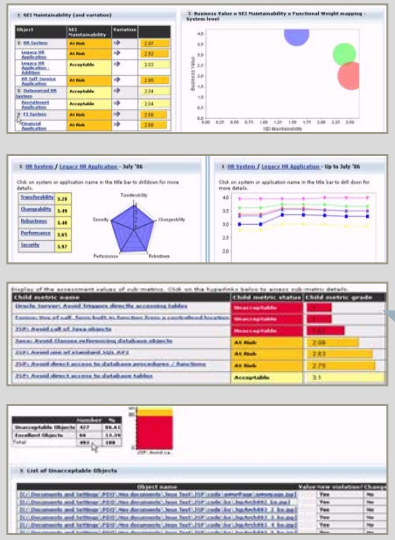
AD Governance Dashboard

Management Visibility



To assess, monitor, and improve applications, development teams and 3rd Party delivery teams

Drill-down to Action



Overview…

Portfolio

Apps

Modules

Objects

Health factors

Sub-metrics

Rules

Compliance

… to remediation

First Annual Report : Data Highlights

The Sample

- Companies: 74
- Applications: 288
- 108M Lines of Code (3.4 M Backfired Function Points)

Key Industries

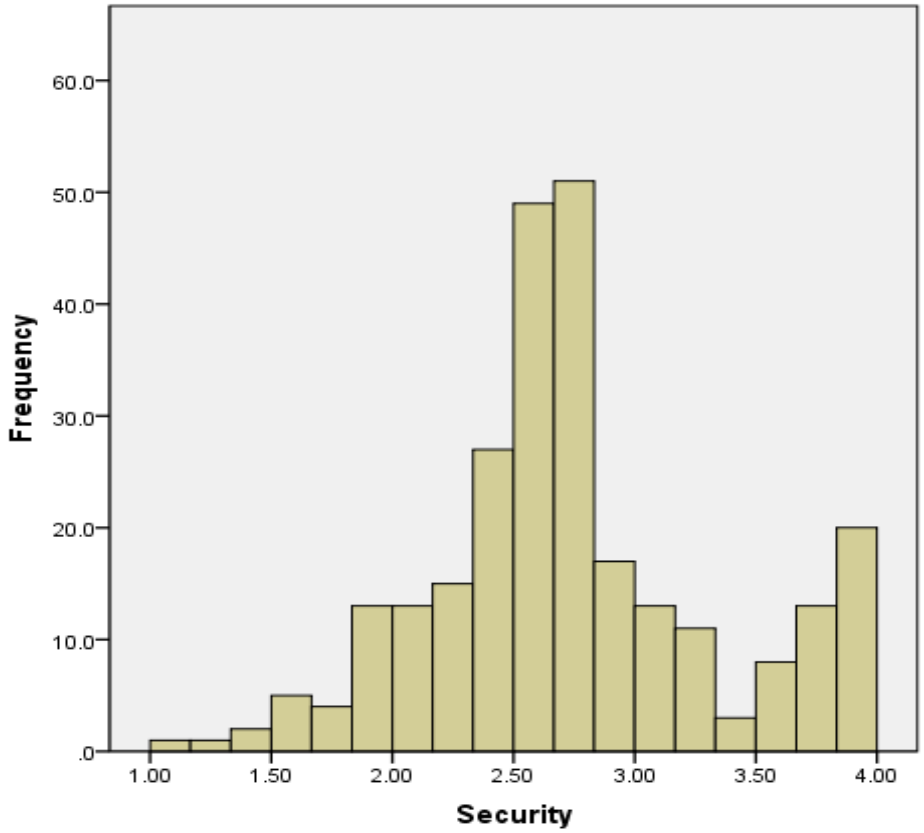
- Energy & Utilities
- Financial Services
- Insurance
- IT & Business Consulting
- Manufacturing
- Government
- Telecommunication
- Software ISV

Key Technologies

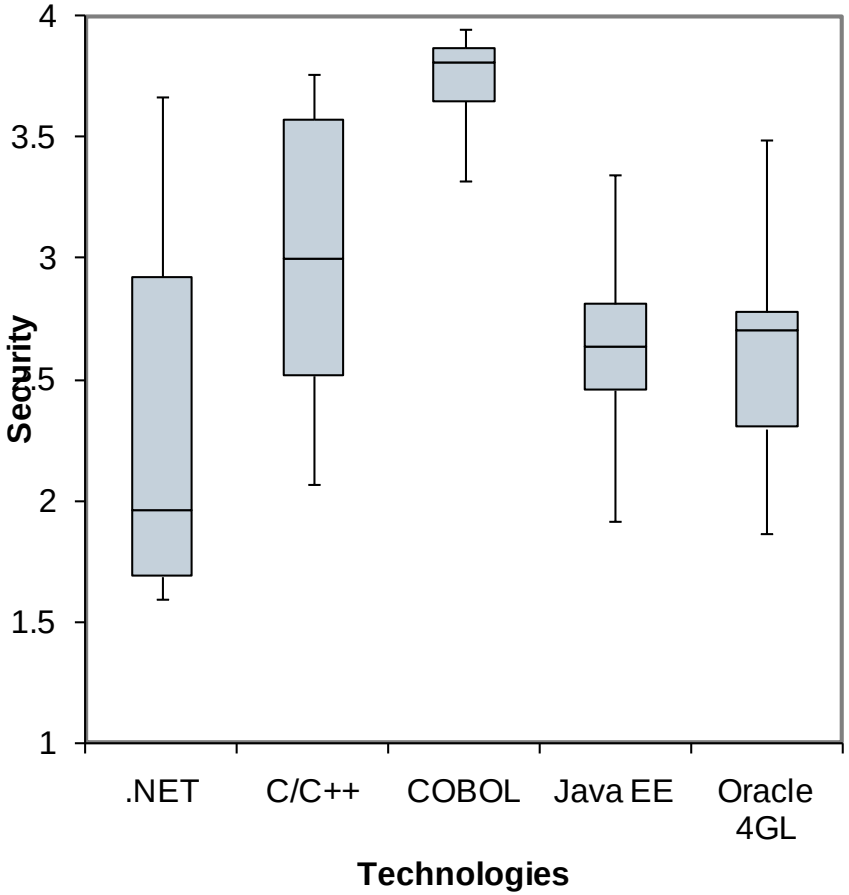
- .NET
- COBOL
- Java EE
- C/C++
- Oracle 4GL
- ABAP

Key Finding 1: Higher Security Scores for COBOL

Distribution of Security Scores.



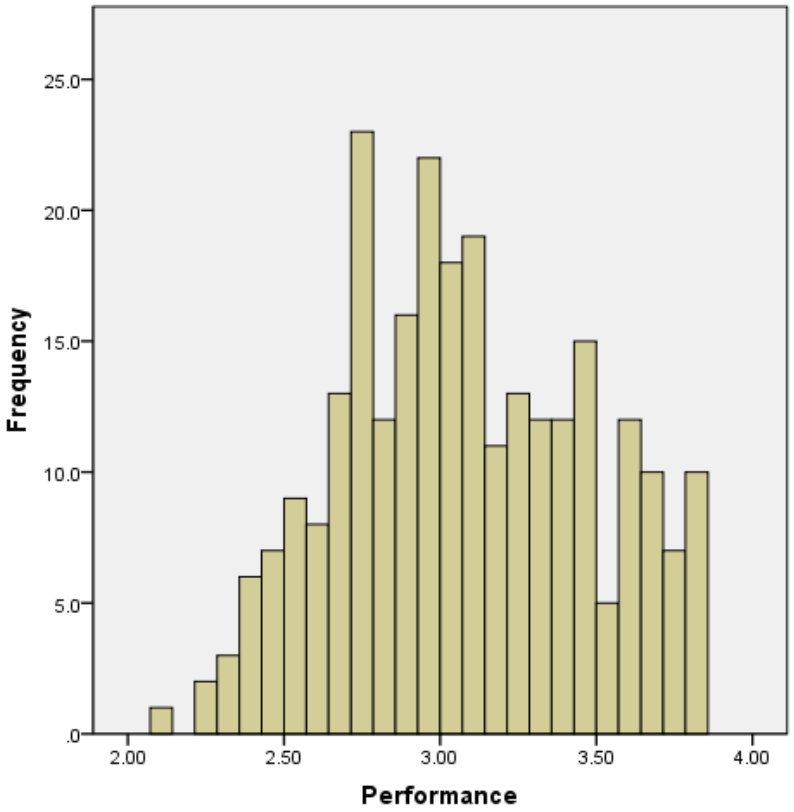
Security scores by language.



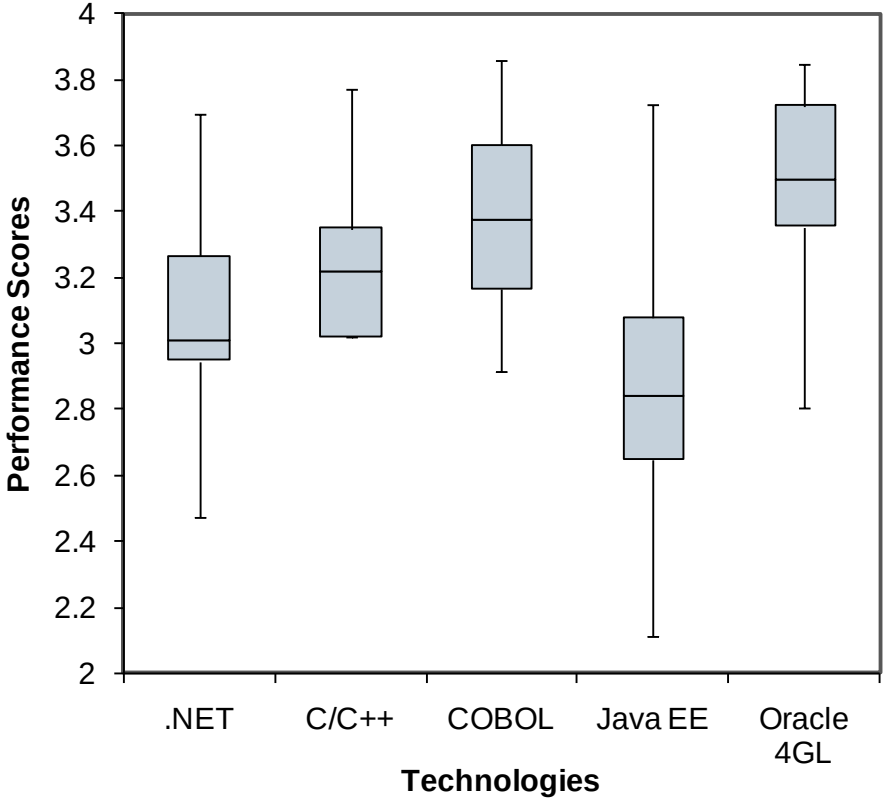
- Bimodal distribution of security scores indicate two types of apps
- Apps with security scores are predominantly from Financial Services

Key Finding 2: Performance Scores Lower in Newer Languages

Distribution of Performance Scores.



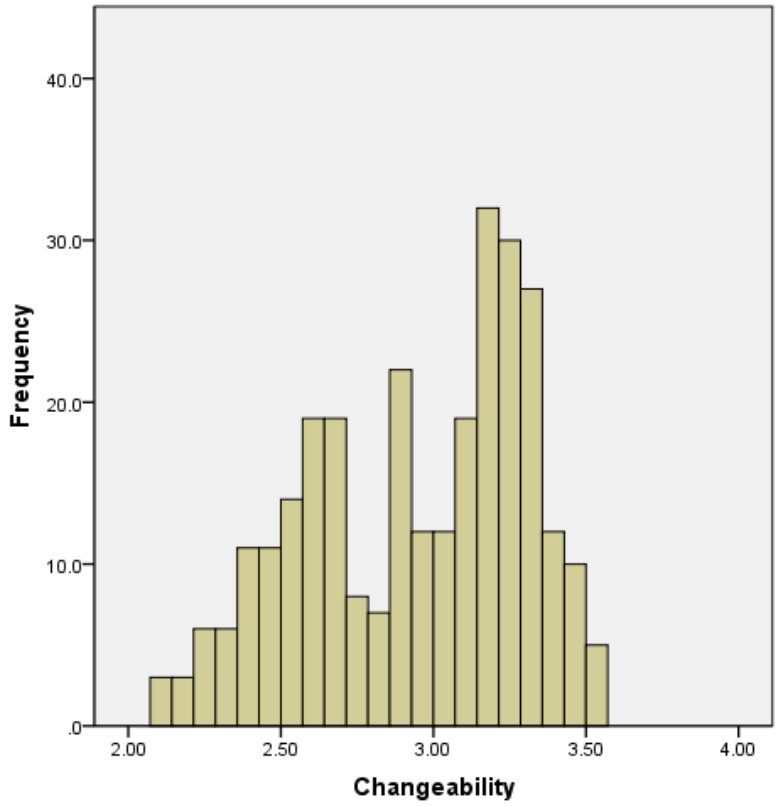
Performance scores by language.



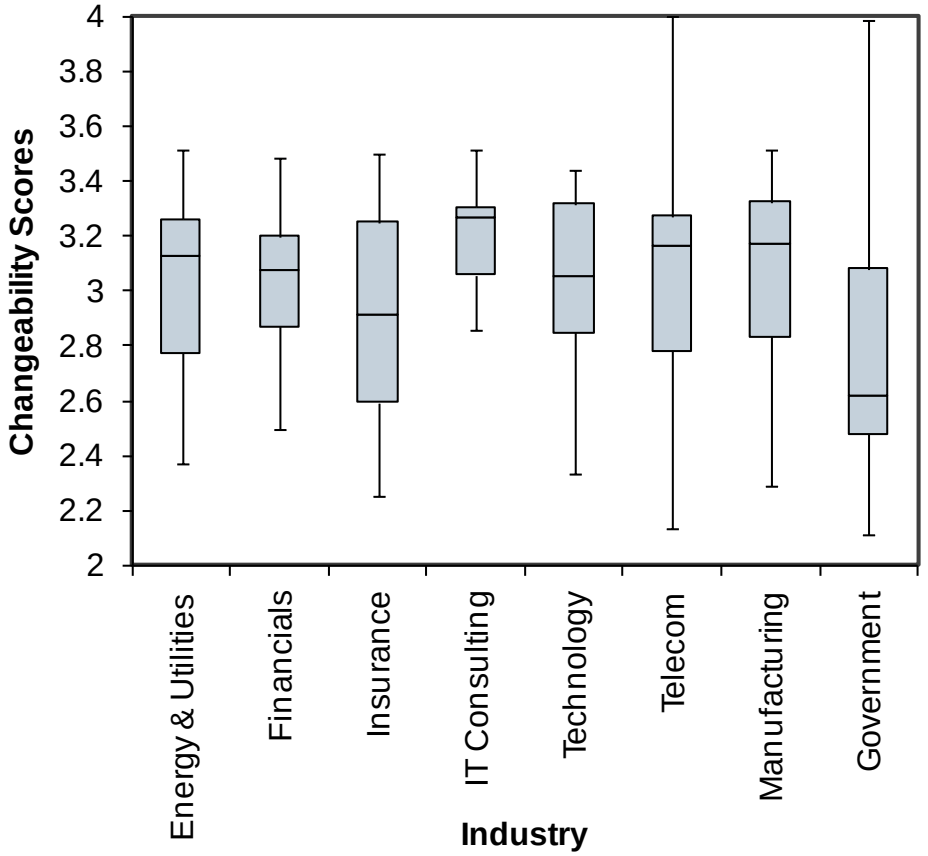
- Performance distribution is skewed towards higher scores in general
- Newer technologies show lower performance scores

Key Finding 3: Changeability Scores Lowest in Government Sector

Distribution of Changeability Scores.

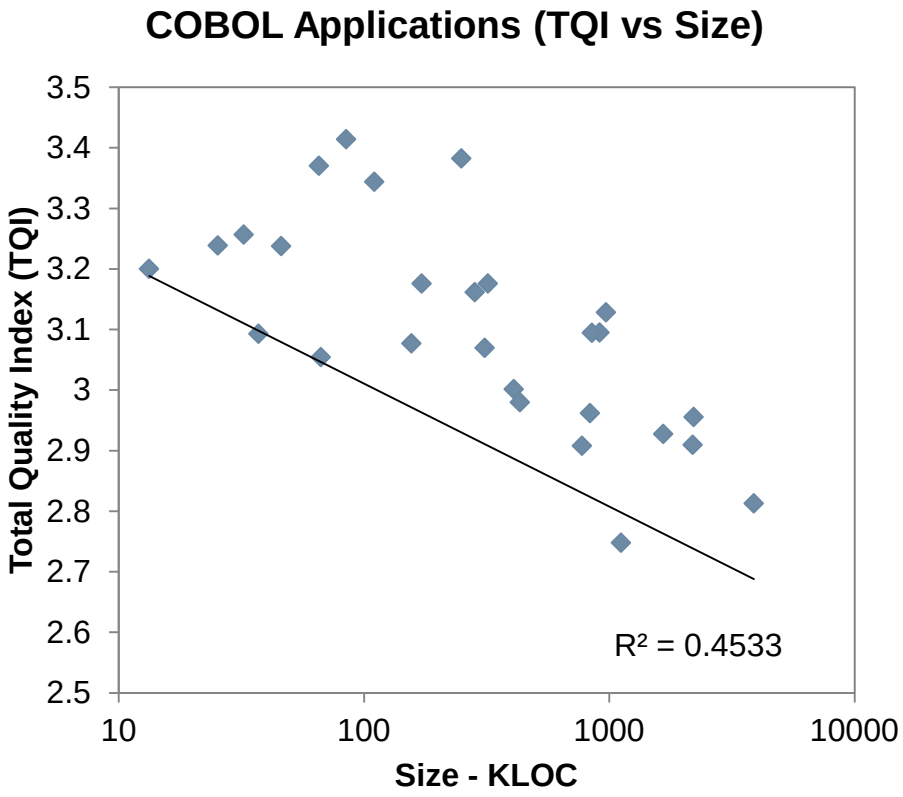


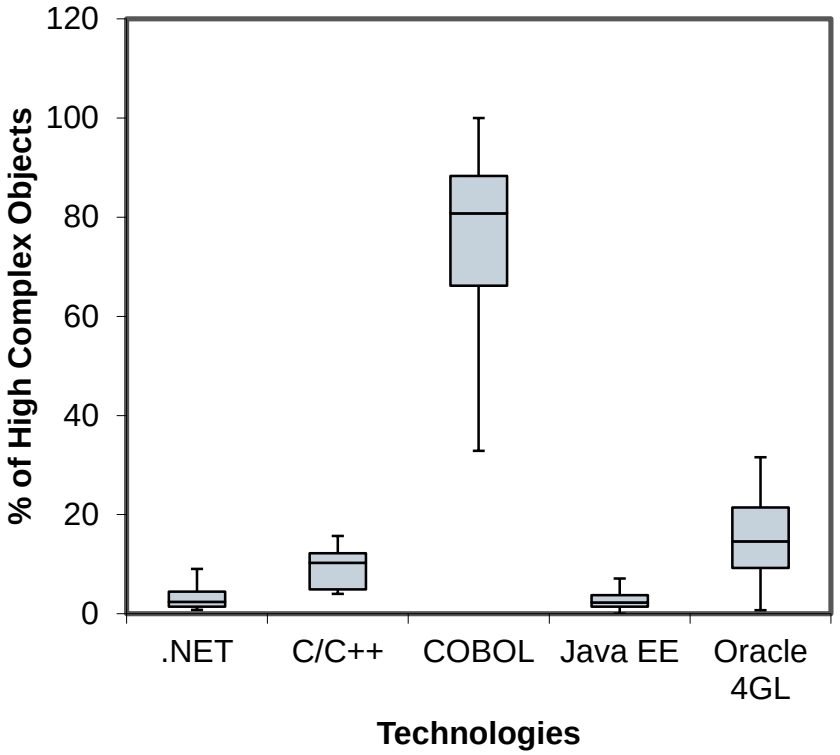
Changeability scores by industry



- Applications in government sector show poor changeability
- Government sector also outsources 75% of apps compared to 50% in private sector.

Key Finding 4: Modularity Minimizes the Effect of Size on Quality





- Except for COBOL applications size has no impact on the quality of applications
- Modularity on the other hand seems to have direct impact on quality

CISQ — An Industry Response

Carnegie Mellon Software Engineering Institute

OBJECT MANAGEMENT GROUP

Co-sponsorship

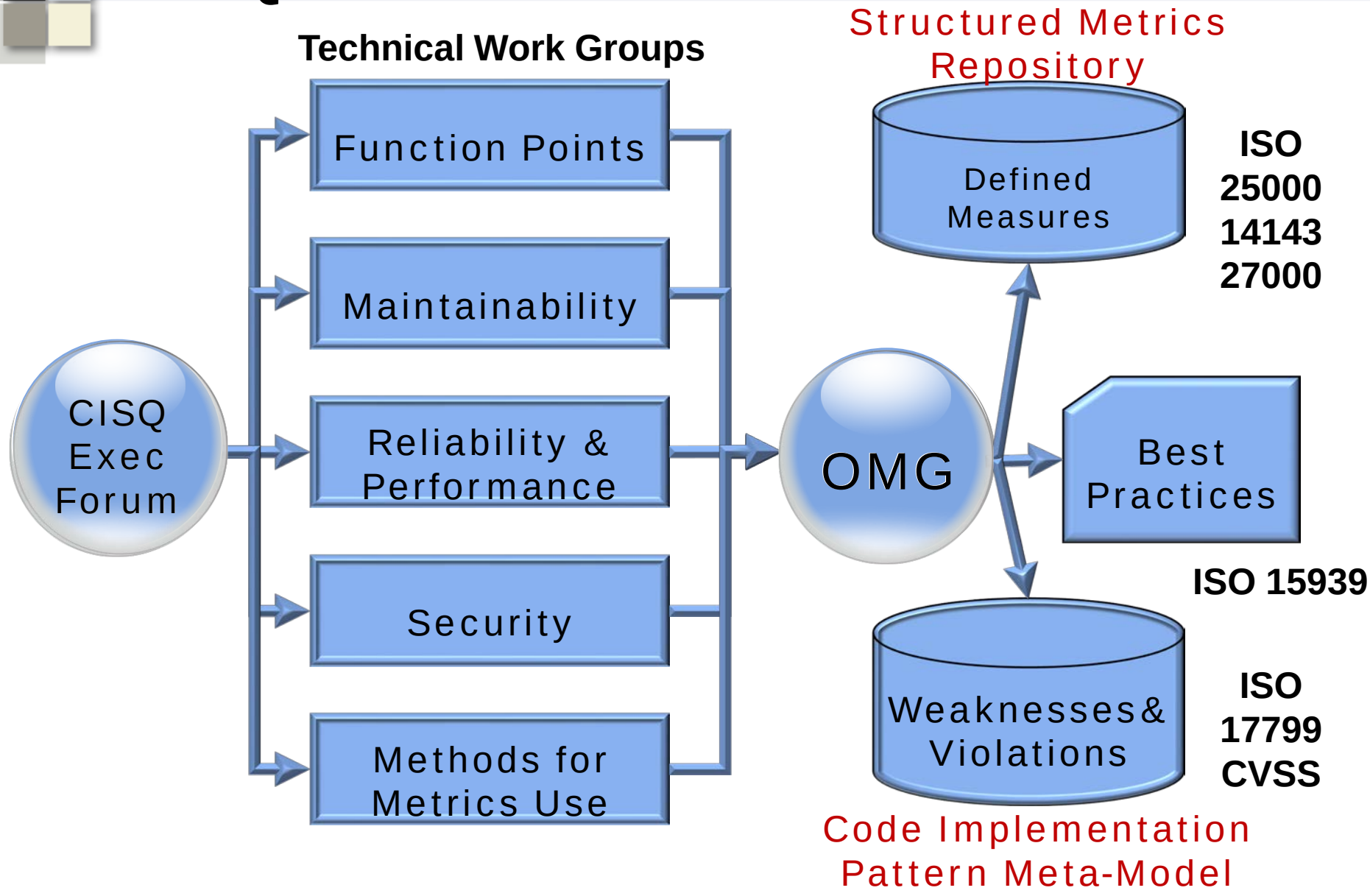
IT Executives → **CISQ** ← Technical experts

IBM, AXA, UBS, McKESSON, TATA, Atos Origin, GM, Aldata, Alcatel·Lucent, outsystems About Agility, TURKCELL TEKNOLOJİ, Capgemini, AMADEUS, steria, DNV, HCL, CSC, DCG, Cognizant, U.S. Department of Homeland Security, Sopra group, 3i Infotech, CAST

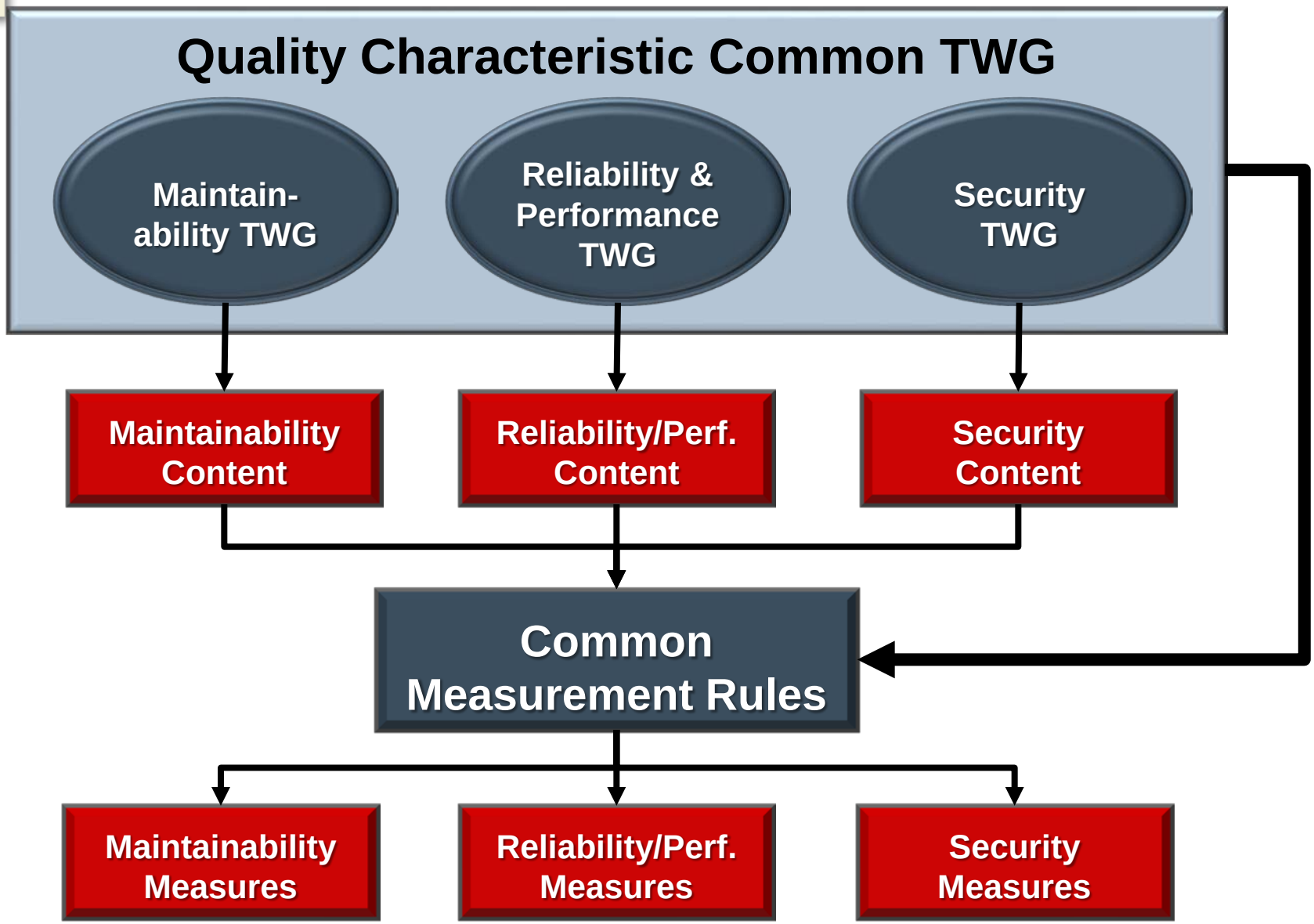
Initial CISQ Objectives

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 Standards Process



Technical Work Group Operations



ISO 25000 Quality Model

Starting point for CISQ work

- *Defines quality characteristics and subcharacteristics*
- *CISQ to define quality attributes and measurable elements*