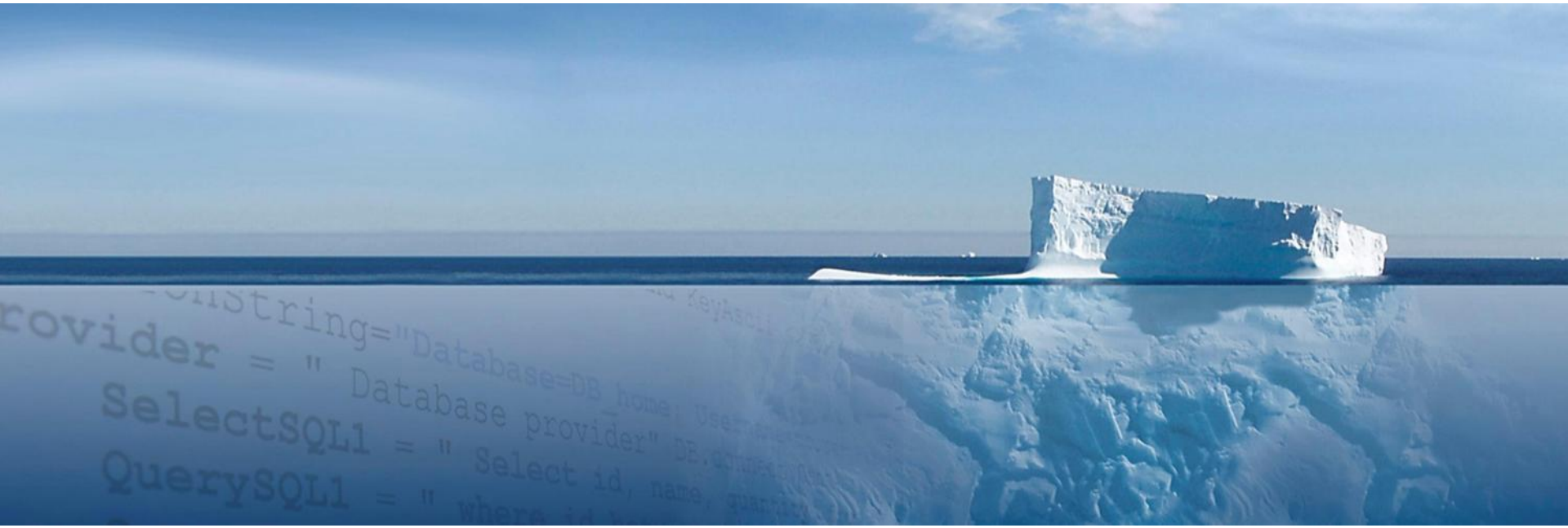
CAST

ACHIEVE INSIGHT. DELIVER EXCELLENCE.

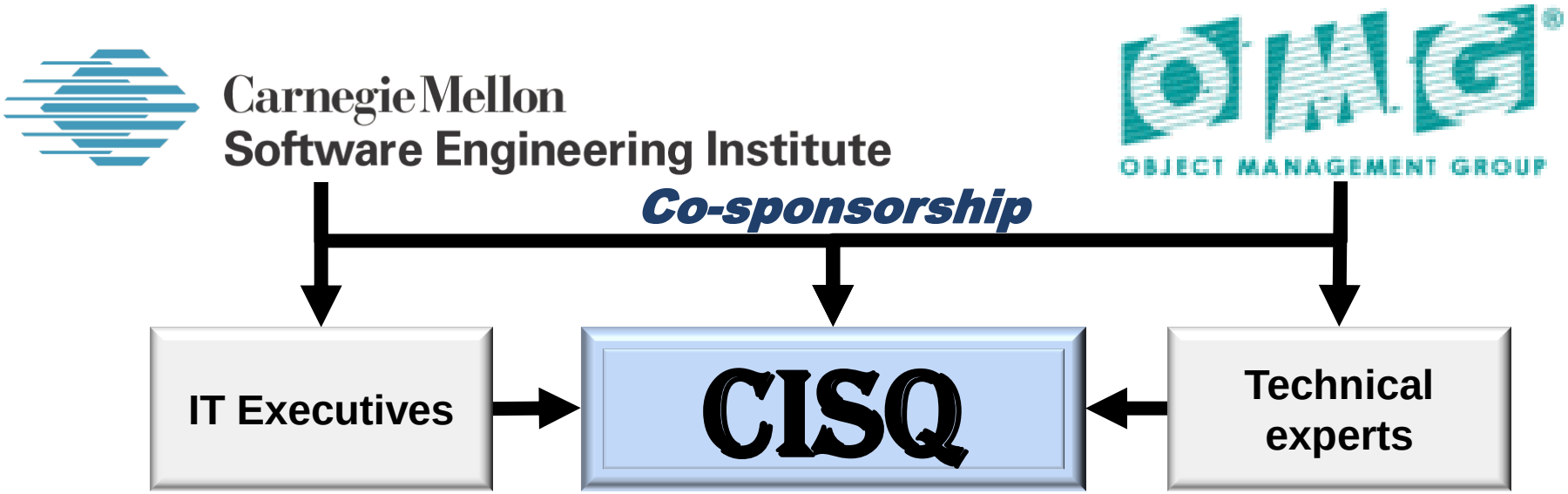


Integrating CISQ Size and Quality Measures into Contractual SLAs

Dr. Bill Curtis

SVP & Chief Scientist, CAST Research Labs
Director, Consortium for IT Software Quality

Consortium for IT Software Quality



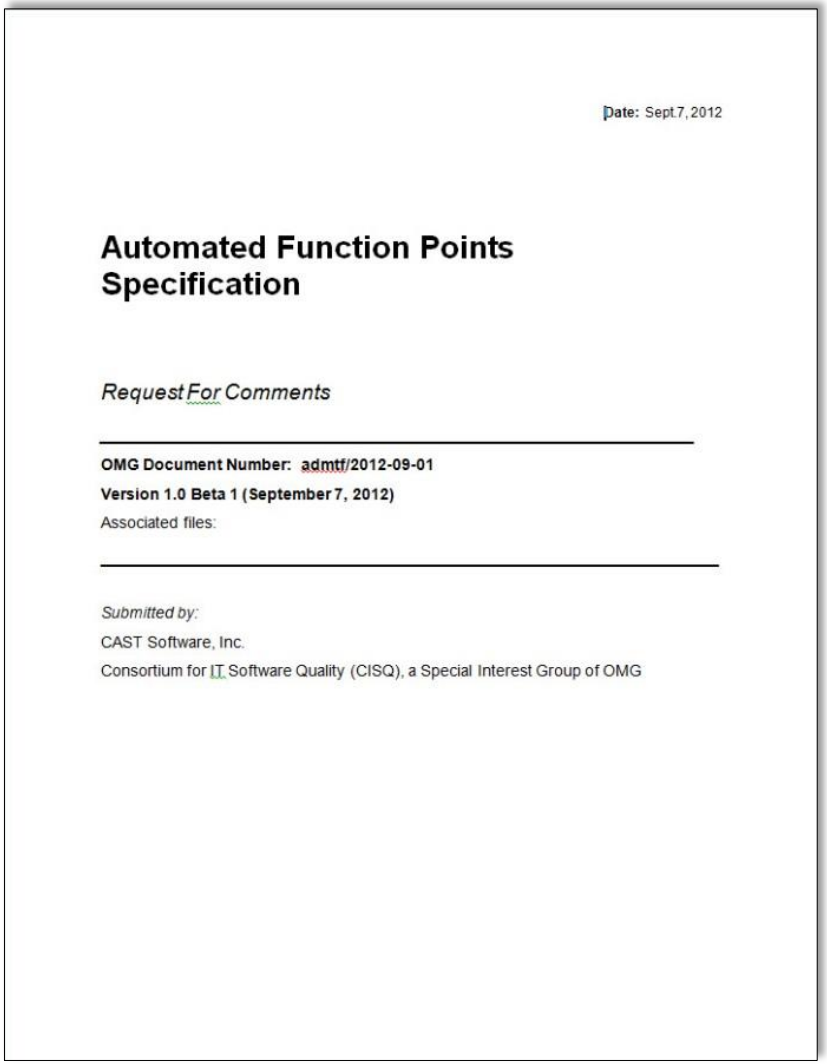
CISQ sponsors

Capgemini

HUAWEI

CAST

Recent CISQ Products



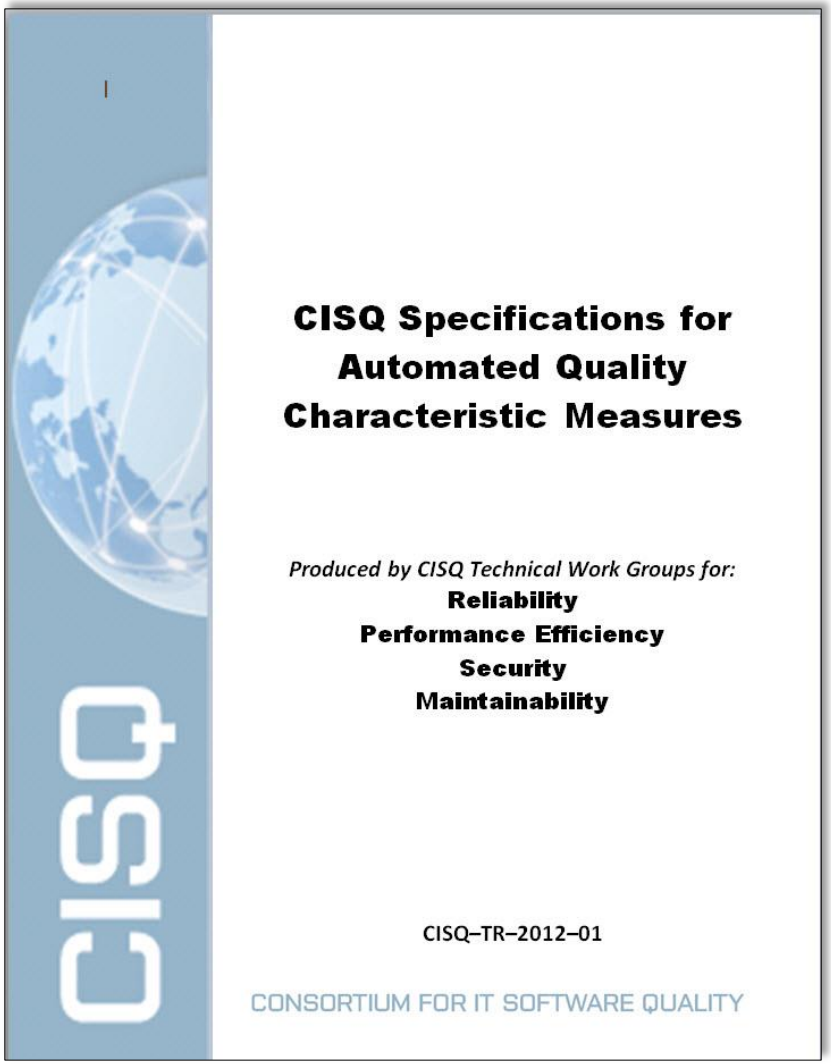
Date: Sept.7, 2012

Automated Function Points Specification

Request For Comments

OMG Document Number: admtf/2012-09-01
Version 1.0 Beta 1 (September 7, 2012)
Associated files:

Submitted by:
CAST Software, Inc.
Consortium for IT Software Quality (CISQ), a Special Interest Group of OMG



CISQ

CISQ Specifications for Automated Quality Characteristic Measures

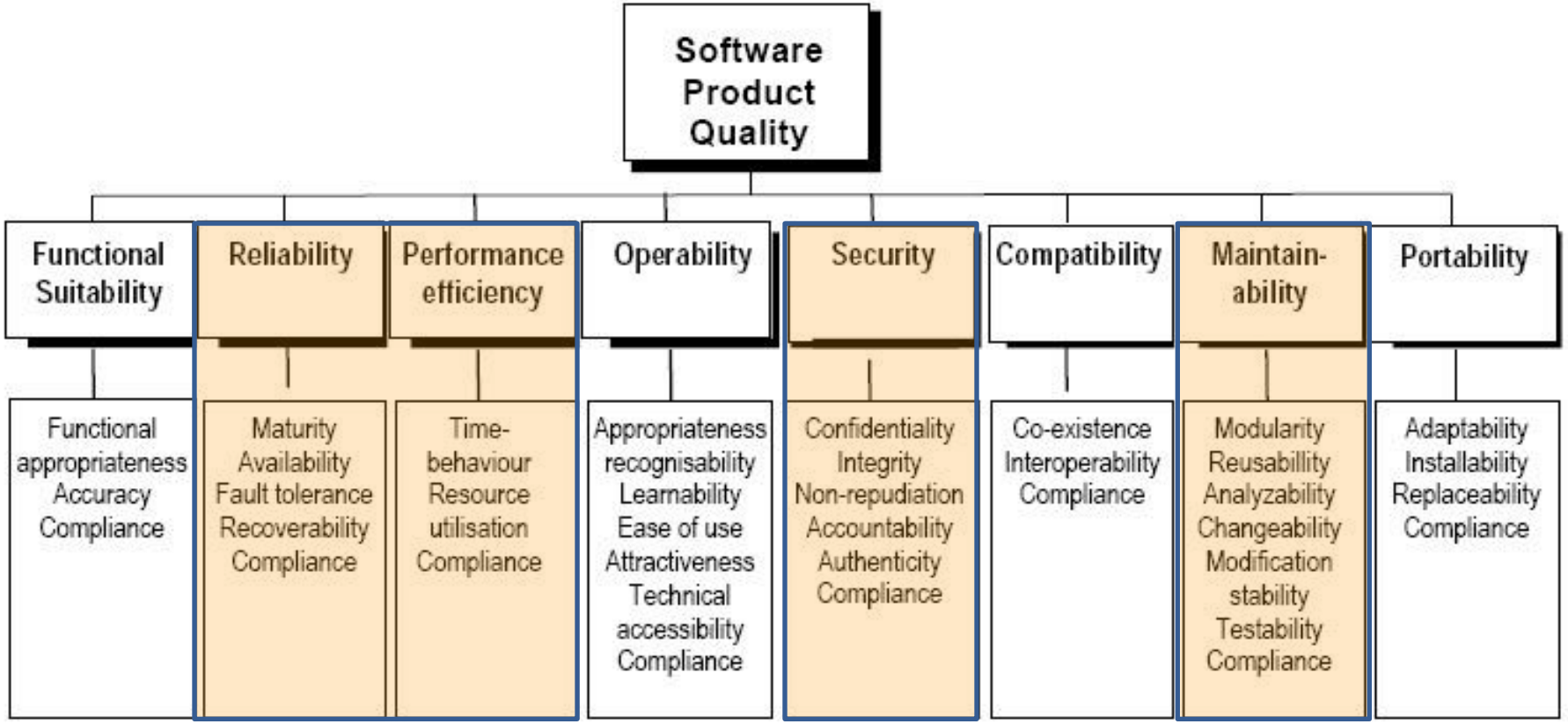
Produced by CISQ Technical Work Groups for:
Reliability
Performance Efficiency
Security
Maintainability

CISQ–TR–2012–01

CONSORTIUM FOR IT SOFTWARE QUALITY

CISQ Measures and ISO 25010

- **Starting point for CISQ work**
  - **Defines quality characteristics and sub-characteristics**
  - **CISQ to define quality attributes and measurable elements**



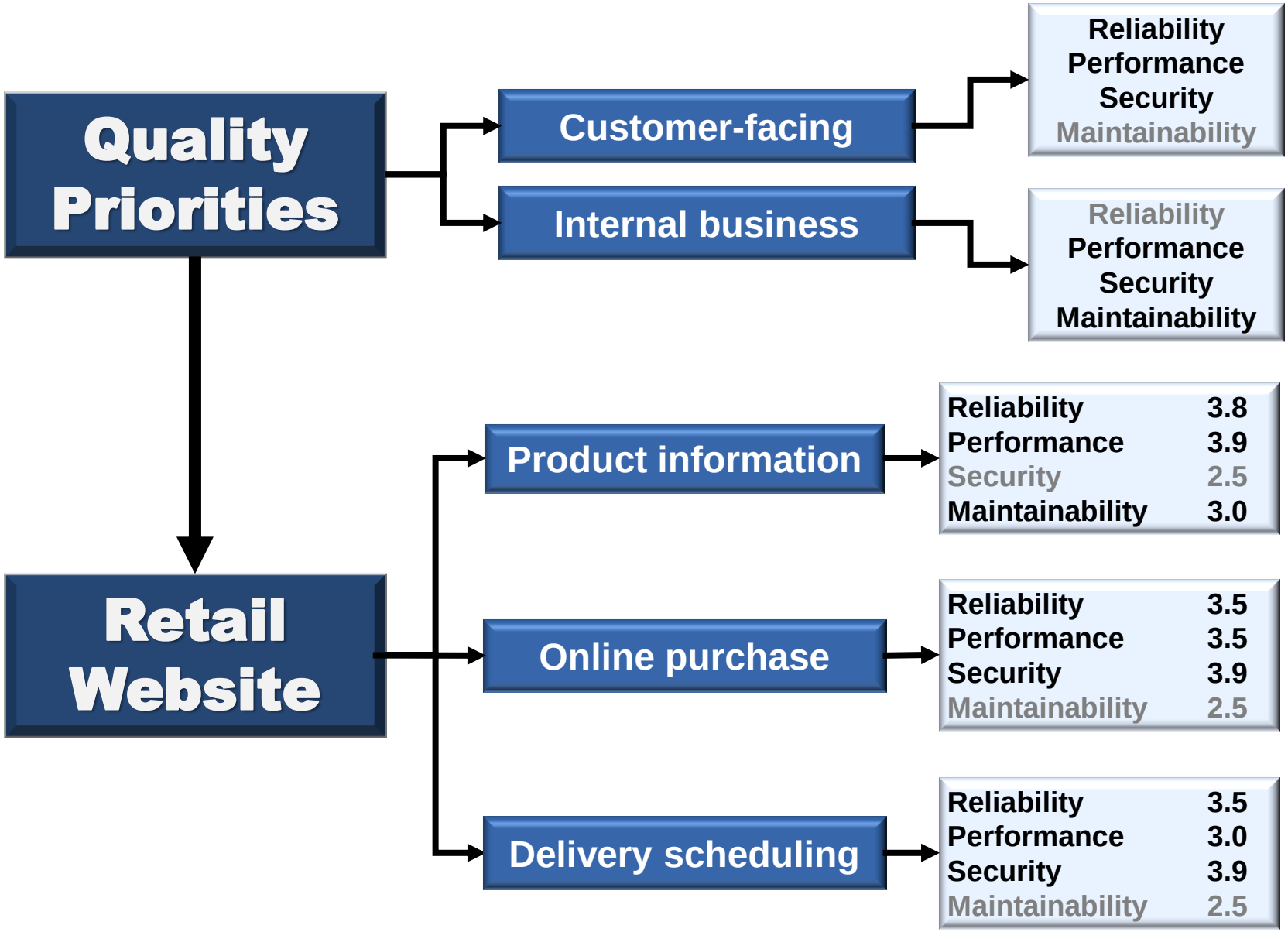
Example Measure for Reliability

Quality Issue	Quality Rule	Quality Measure Element
Issue 1: Inconsistent or incomplete handling of errors and exceptions leads to inaccurate identification and inadequate response to errors	**Rule 1:** Exception handling blocks such as Catch and Finally blocks must not be empty.	**Measure 1:** # of exception handling blocks such as Catch and Finally blocks that are empty **Measure 2:** # of generic exceptions thrown and caught
	Rule 2: Methods, procedures and functions doing Insert, Update, Delete, Create Table or Select must include error management (check of database error variables or exception handling).	**Measure 3:** # of functions doing Insert, Update, Delete, Create Table, and Select that do not include error management capabilities
Issue 2: Some coding weaknesses result in unexpected and faulty behaviors	**Rule 3:** Classes that implement a serializable interface must also implement a serializable method and subfields within the object that are serializable.	**Measure 4:** # of classes that implement a serializable interface must also implement a serializable method **Measure 5:** # of classes that have

Recommendations for Using Measures in SLAs

1. **Set structural quality objectives**
2. **Measure unacceptable violations**
3. **Use a common vocabulary**
4. **Measure quality at system level**
5. **Define roles and responsibilities**
6. **Follow a measurement process**
7. **Evaluate contract deliverables**
8. **Use rewards and penalties wisely**

1—Set Structural Quality Objectives



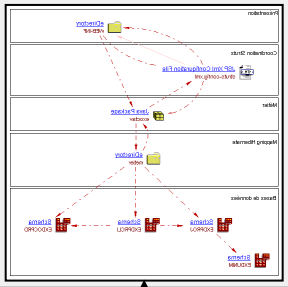
2—Measure Unacceptable Violations

Parse App Layers → **Analyze Application** → **Detect Violations** → **Measure Quality**

- 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 for other languages

Evaluation of architectural & coding rules

Application meta-data

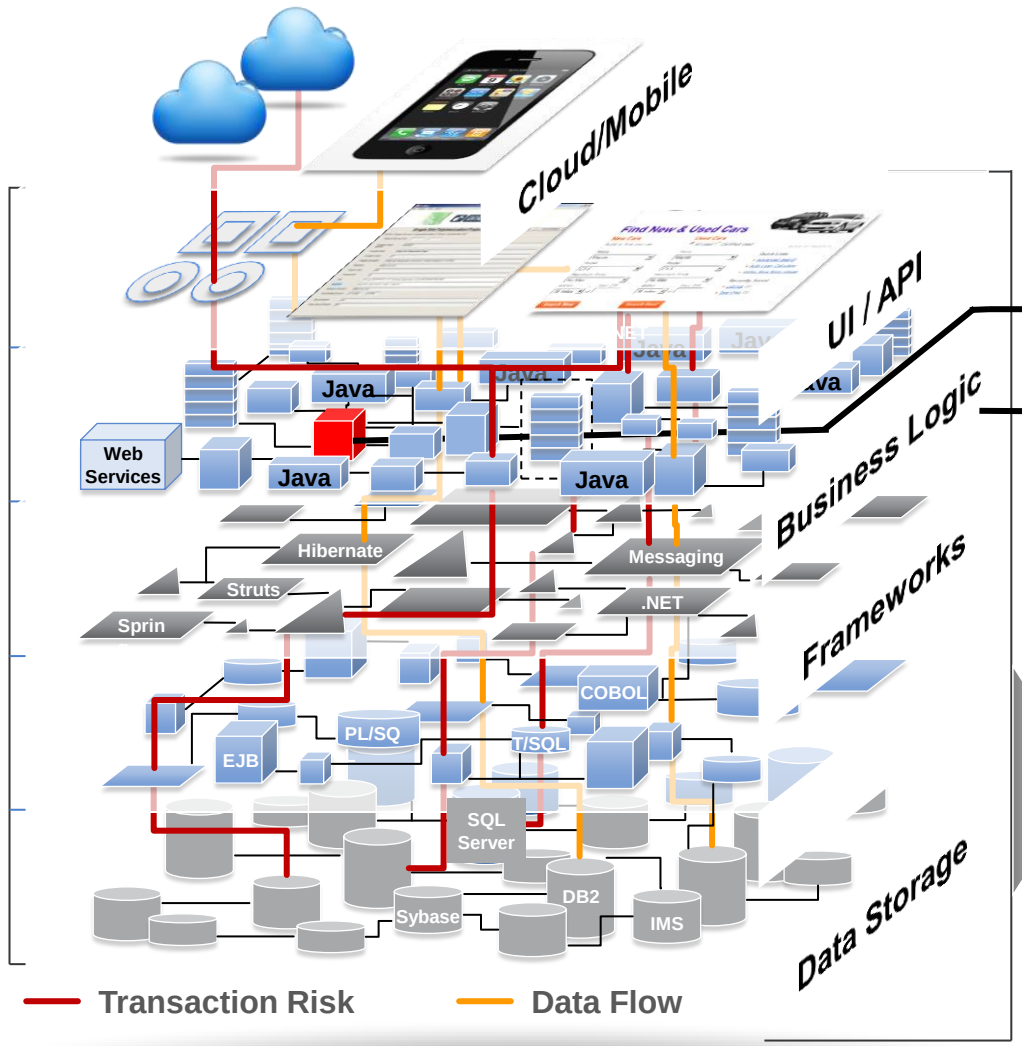


Detect Violations	Measure Quality
Expensive operation in loop Static vs. pooled connections Complex query on big table Large indices on big table	Performance
Empty CATCH block Uncontrolled data access Poor memory management Opened resource not closed	Robustness
SQL injection Cross-site scripting Buffer overflow Uncontrolled format string	Security
Unstructured code Misuse of inheritance Lack of comments Violated naming convention	Transferability
Highly coupled component Duplicated code Index modified in loop High cyclomatic complexity	Changeability

3—Use a Common Vocabulary

Term	Definition
Software Quality	Software quality will be measured by the CISQ Quality Characteristic measures for Reliability, Security, Performance Efficiency, and Maintainability
Application Size	Application size will be measured by the CISQ specification for Automated Function Points. The work performed on an application will be measured by the CISQ Enhanced Function Point measure
Violations	Application source code that violates a rule incorporated into one of the four CISQ Quality Characteristic measures or a coding standard incorporated into an SLA
Unacceptable Violations	Violations specified in an SLA that must not exist in delivered code. All unacceptable violations must be remediated before delivery will be accepted
Minimum Threshold	Minimum score established in an SLA that must be attained on one or more CISQ Quality Characteristic measures for a delivery to be accepted. Failure to achieve the minimum threshold can result in rejection of the delivery or financial penalties
Expected Target	The score established in an SLA that should be attained on one or more CISQ Quality Characteristic measures that the supplier should seek to achieve and sustain over releases. A schedule over several releases may be established for achieving the expected target

4—Measure Quality at 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

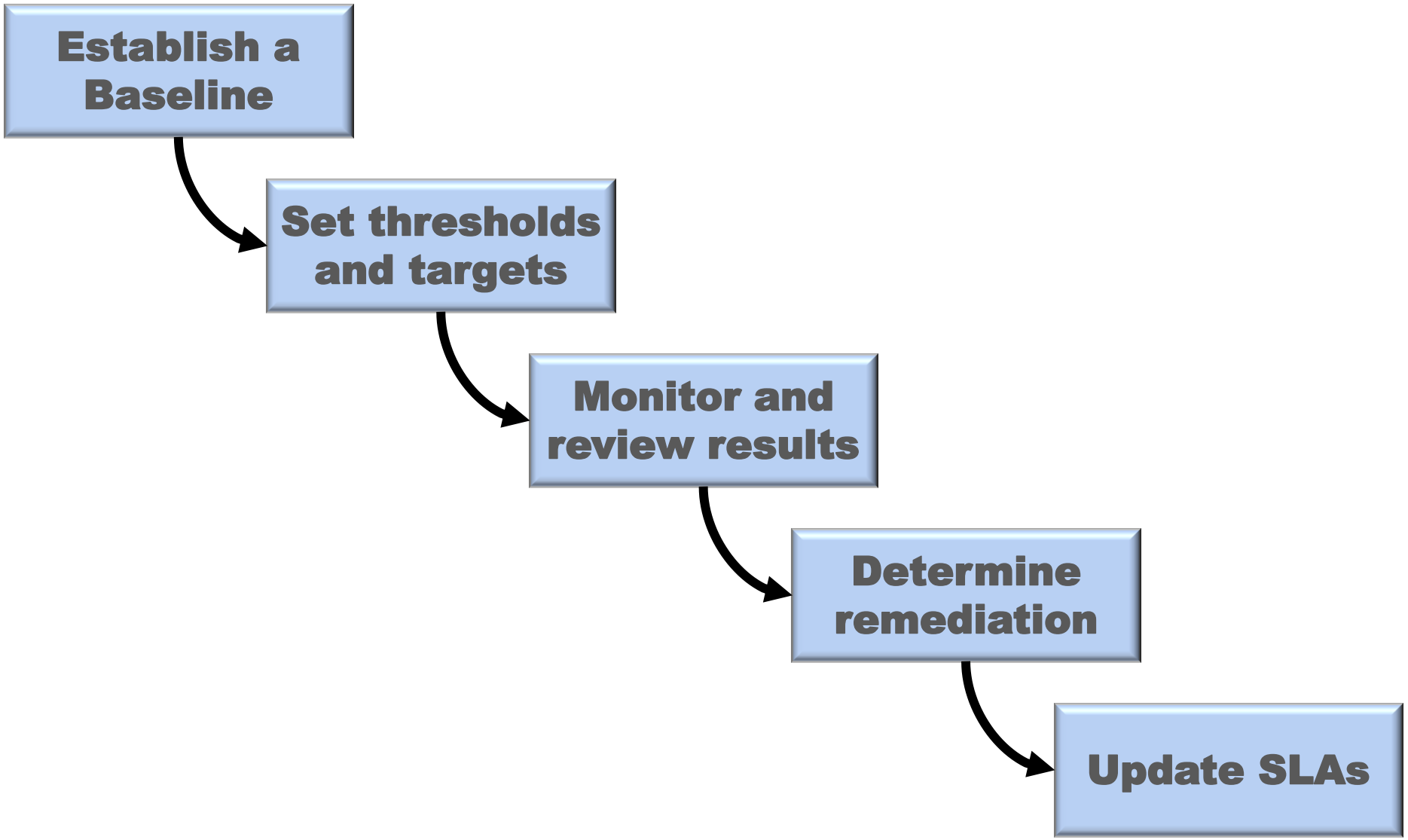
3 System Level

- 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

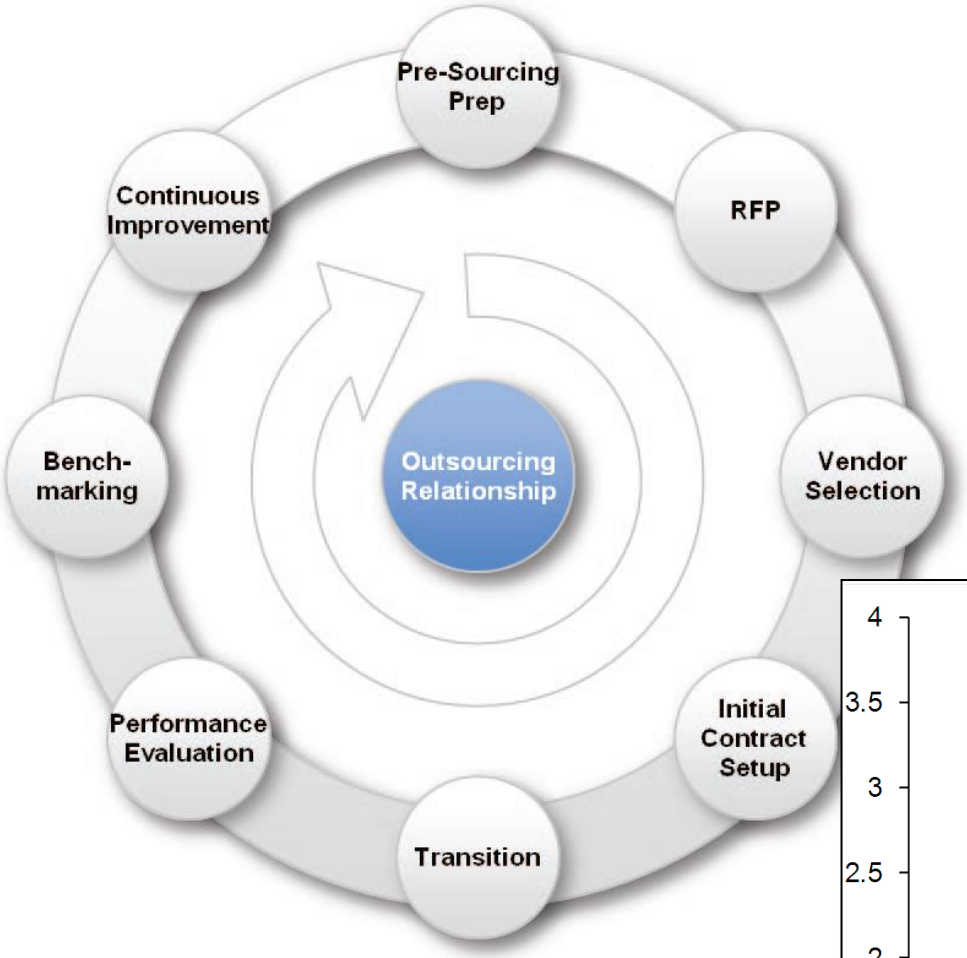
5—Define Roles and Responsibilities

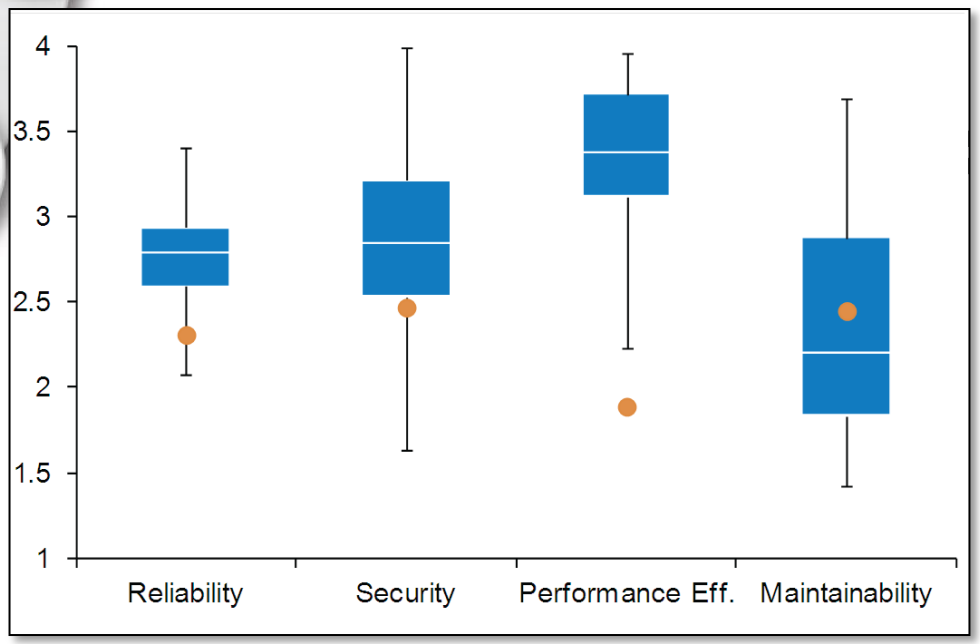
Customer	Supplier
For each application under contract, the company should develop SLAs in consultation with the supplier that clearly define the minimum threshold and expected target of measures, as well as all unacceptable violations that may not be in the source code at delivery.	The supplier should make all developers, testers, and other staff involved with the application aware of the SLA requirements and how they are to be achieved and sustained.
In their SLAs the company should clearly define the measures to be used in assessing these thresholds and targets and how the scores will be determined.	For each application the supplier should commit to meet the minimum threshold and provide an action plan for achieving the expected target scores defined in the SLAs.
They should conduct a defined analysis and measurement process when code is delivered and provide a report to the supplier that clearly describes the results and any actions expected of the supplier.	The supplier should conduct quality assurance activities during the development period to ensure that SLA agreements will be achieved.
Customers should host a post-analysis meeting with a supplier representative to discuss measurement results and plan for future actions and expectations regarding application size and structural quality.	Upon request, the supplier should deliver whole source code including SQL structure definition files of the application to support an application audit by the customer, even if the new release does not modify all components of the application.
	The supplier should meet with the customer to discuss results of analysis and measurement activities, to identify any remedial action required immediately, and to plan for future actions and expectations regarding application size and structural quality.

6—Follow a Measurement Process



7—Evaluate Contract Deliverables

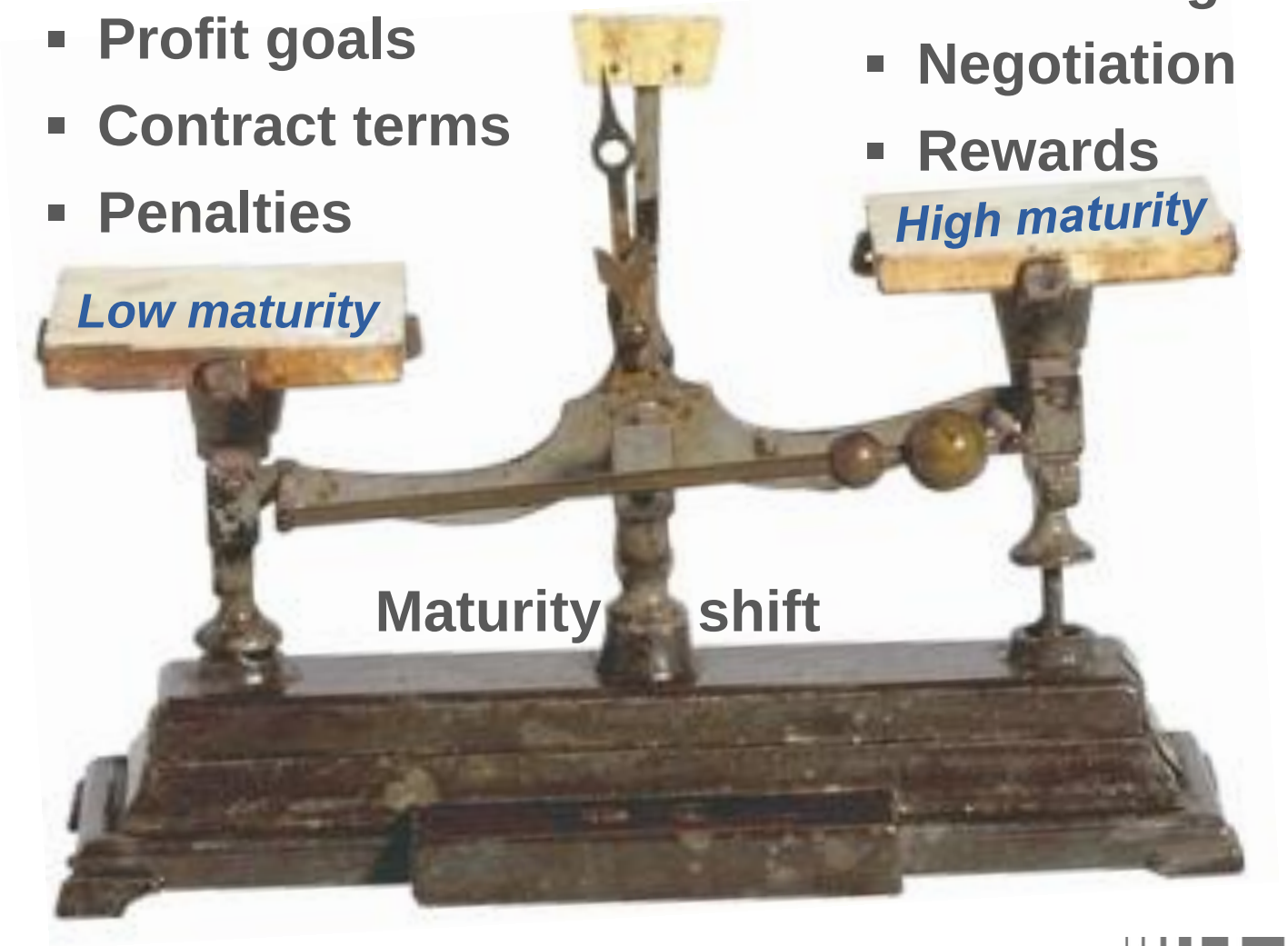




8—Use Rewards and Penalties Wisely

- Vendor
- Profit goals
- Contract terms
- Penalties

- Partnership
- Common goals
- Negotiation
- Rewards



New CISQ Website — Free Membership