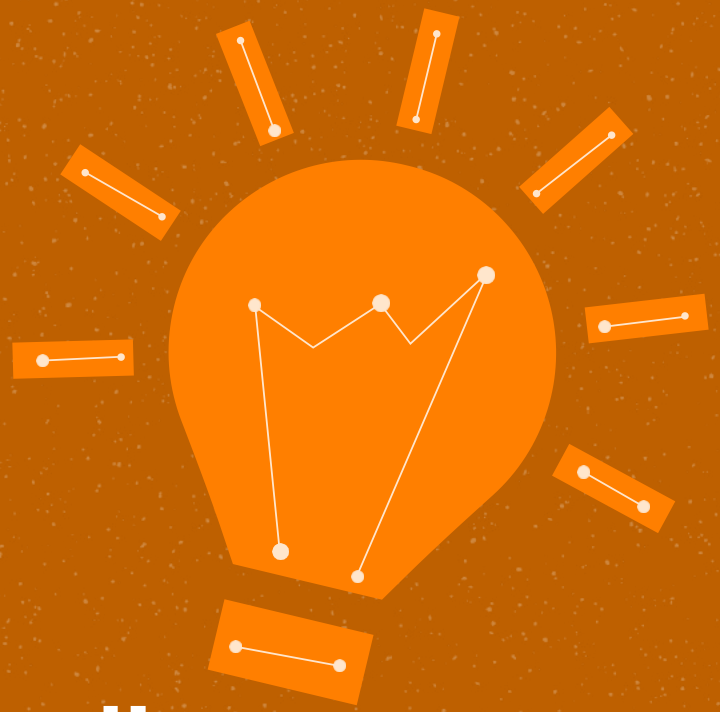
Puglia

OSSERVAZIONI SUL FUTURO



La Qualità del software come fattore di successo per una trasformazione digitale sostenibile della PA

Michele Slocovich

Bari, 19 10 2022

NUOVA FIERA DEL LEVANTE

UNIONE EUROPEA

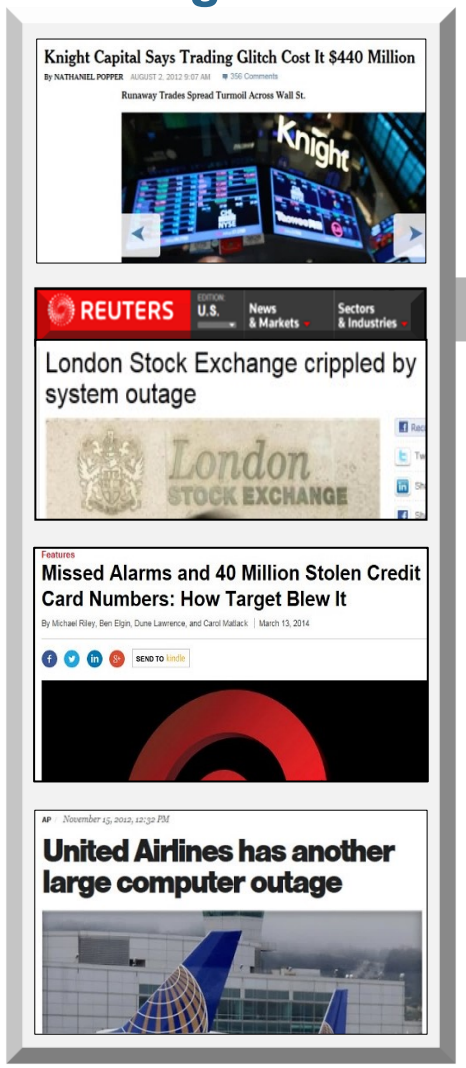
REPUBBLICA ITALIANA

PUGLIA FESR·FSE 2014/2020
Il futuro alla portata di tutti

REGIONE PUGLIA

The Era of Nine-Digit Defects

Nine Digit Defects



now affect

- Board of Directors
- CEO, COO, CFO
- Business VPs
- Corporate Auditors
- CIO

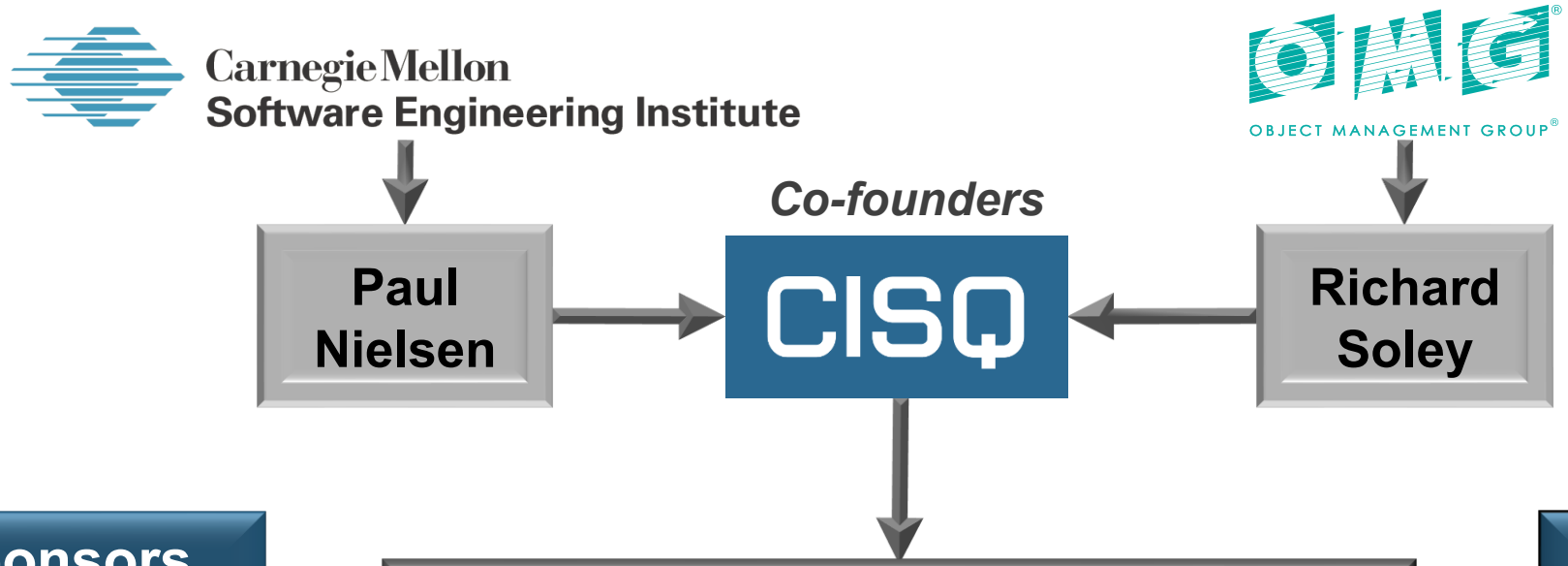
accountable for

- Governance
- Risk management
- Business Continuity
- Brand protection
- Customer experience

Evaluate Application Risk with CISQ Measures

© 2022 Consortium for Information and Software Quality (CISQ) www.it-cisq.org

What Is CISQ ?



CISQ is chartered to specify measures of software size and quality that can be automated from source code, and promote them through OMG and other international standards organizations

CISQ Sponsors

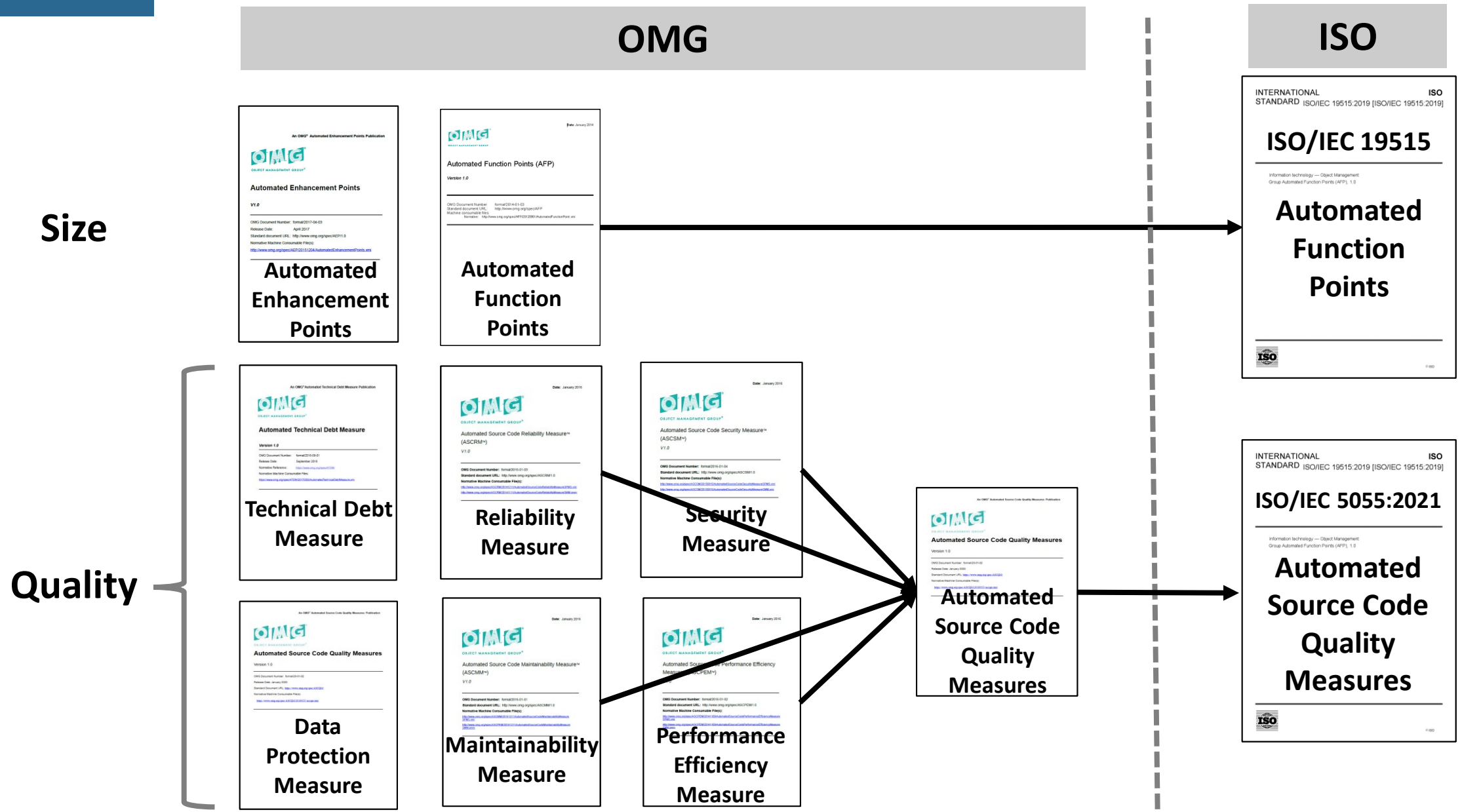
Tech Mahindra
SYNOPSYS
7N
CAST
USC CSSE
SHPI
NORTHROP GRUMMAN
CGI

CISQ Partners

Gartner
QuEST FORUM
FORRESTER
IAOP
USCC
TECHWELL
ITAAC
MAKING SOFTWARE BETTER
ISG
QA

© 2022 Consortium for Information and Software Quality (CISQ) www.it-cisq.org

CISQ/OMG Standards & ISO Fasttrack



© 2022 Consortium for Information and Software Quality (CISQ) www.it-cisq.org

What Is ISO/IEC 5055:2021


INTERNATIONAL STANDARD

ISO/IEC 5055

First edition 2021-03

Information technology — Software measurement — Software quality measurement — Automated source code quality measures

Reference number ISO/IEC 5055:2021(E)

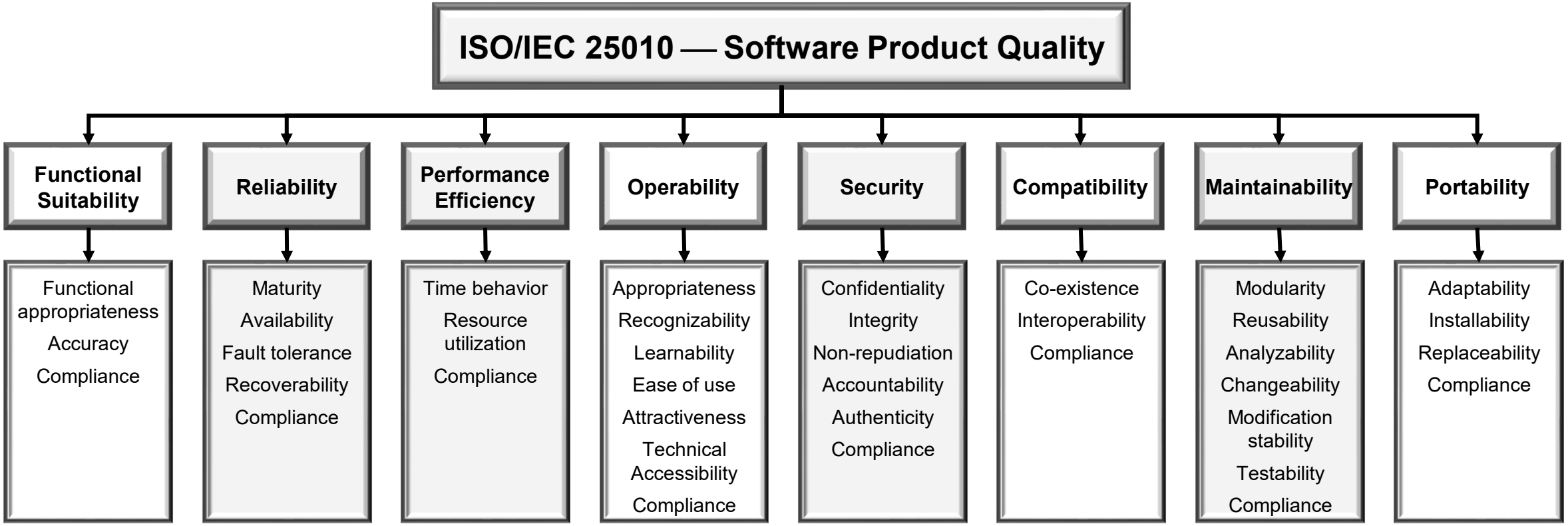
© ISO/IEC 2021

- **Defines measures of the internal, structural quality of software for four ISO/IEC 25010 software quality characteristics:**
  - **Reliability**
  - **Security**
  - **Performance Efficiency**
  - **Maintainability**
- **Measures are calculated from automated detection and counting of severe architectural and coding weaknesses**
- **'Shift-left' structural quality measurement**
- **Can be used for:**
  - **Internal product and process improvement**
  - **System acquisition contracts and acceptance criteria**
  - **Internal and external monitoring and benchmarking**
- **Fasttracked to ISO as a Publicly Available Standard by OMG (Object Management Group) and can be obtained for free at:** https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

© 2022 Consortium for Information and Software Quality (CISQ) www.it-cisq.org

ISO 5055 Supports ISO/IEC 25000 standards

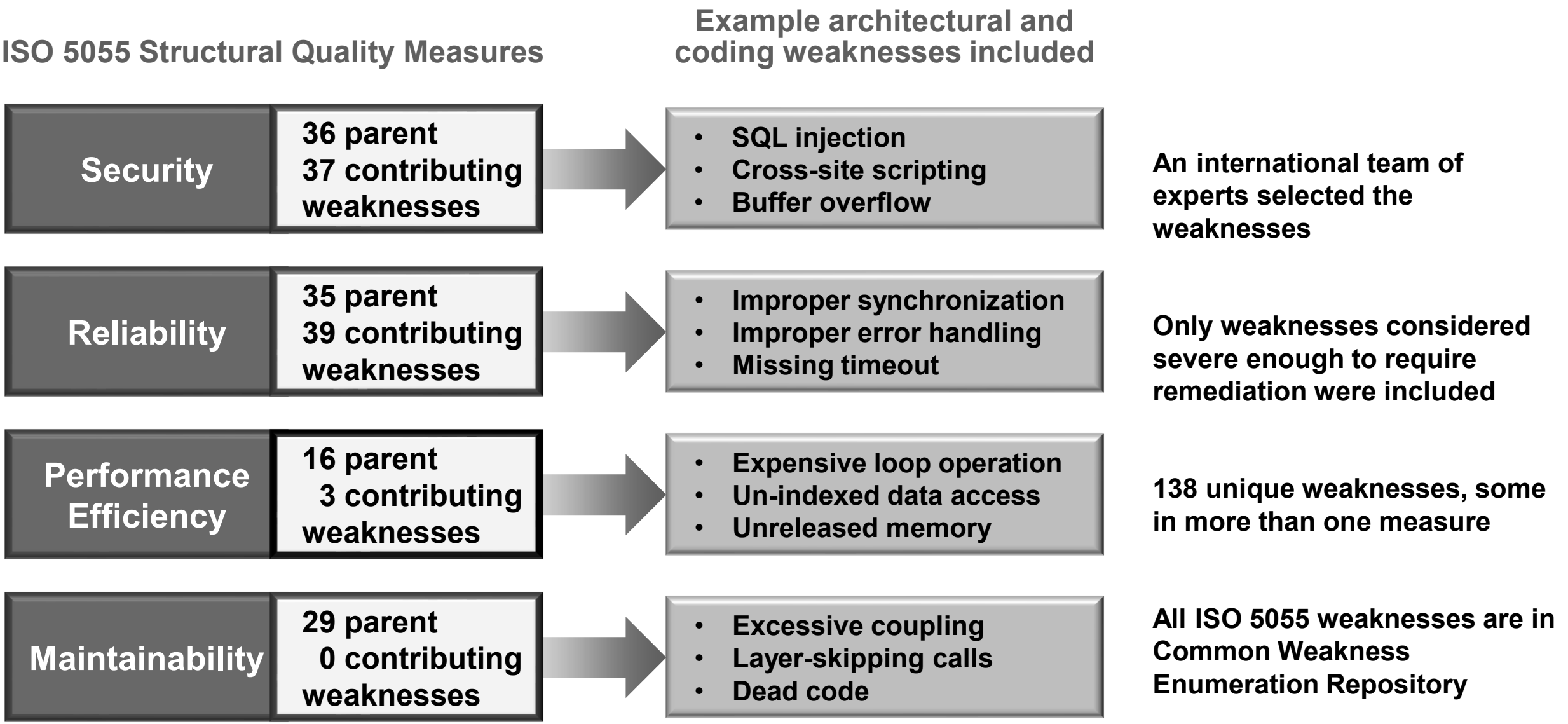
- **ISO/IEC 25010 defines a software product quality model of 8 quality characteristics**
- **ISO/IEC 5055 conforms to four ISO/IEC 25010 quality characteristic definitions**
- **ISO/IEC 25023 defines measures, but not automatable and few the source code level**
- **ISO/IEC 5055 supplements ISO/IEC 25023 with source code level measures**



ISO/IEC 25010 software quality characteristics measured by ISO/IEC 5055 are highlighted in blue

© 2022 Consortium for Information and Software Quality (CISQ) www.it-cisq.org

ISO 5055 Structural Quality Measures



An international team of experts selected the weaknesses

Only weaknesses considered severe enough to require remediation were included

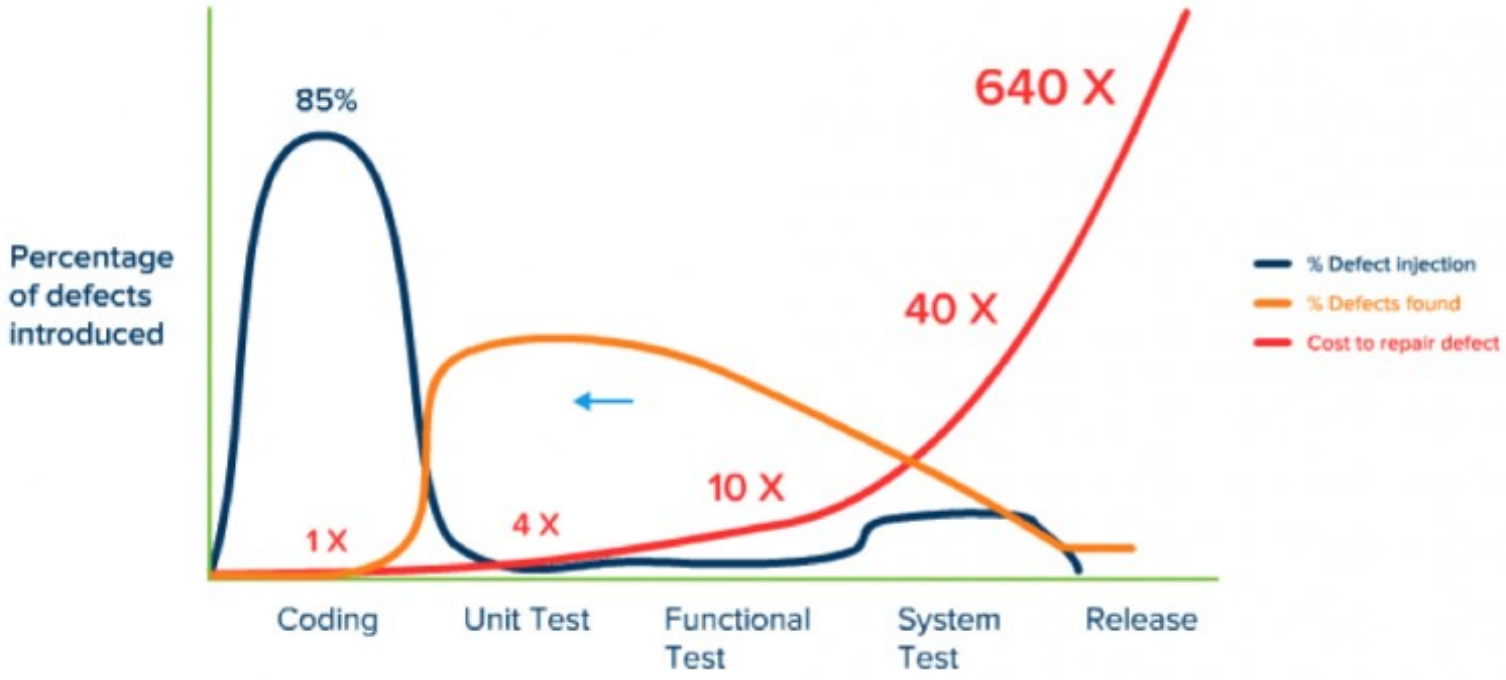
138 unique weaknesses, some in more than one measure

All ISO 5055 weaknesses are in Common Weakness Enumeration Repository

© 2022 Consortium for Information and Software Quality (CISQ) www.it-cisq.org

Rationale: the earliest findings, the lower cost

‘Shift Left’ can dramatically reduce the impact

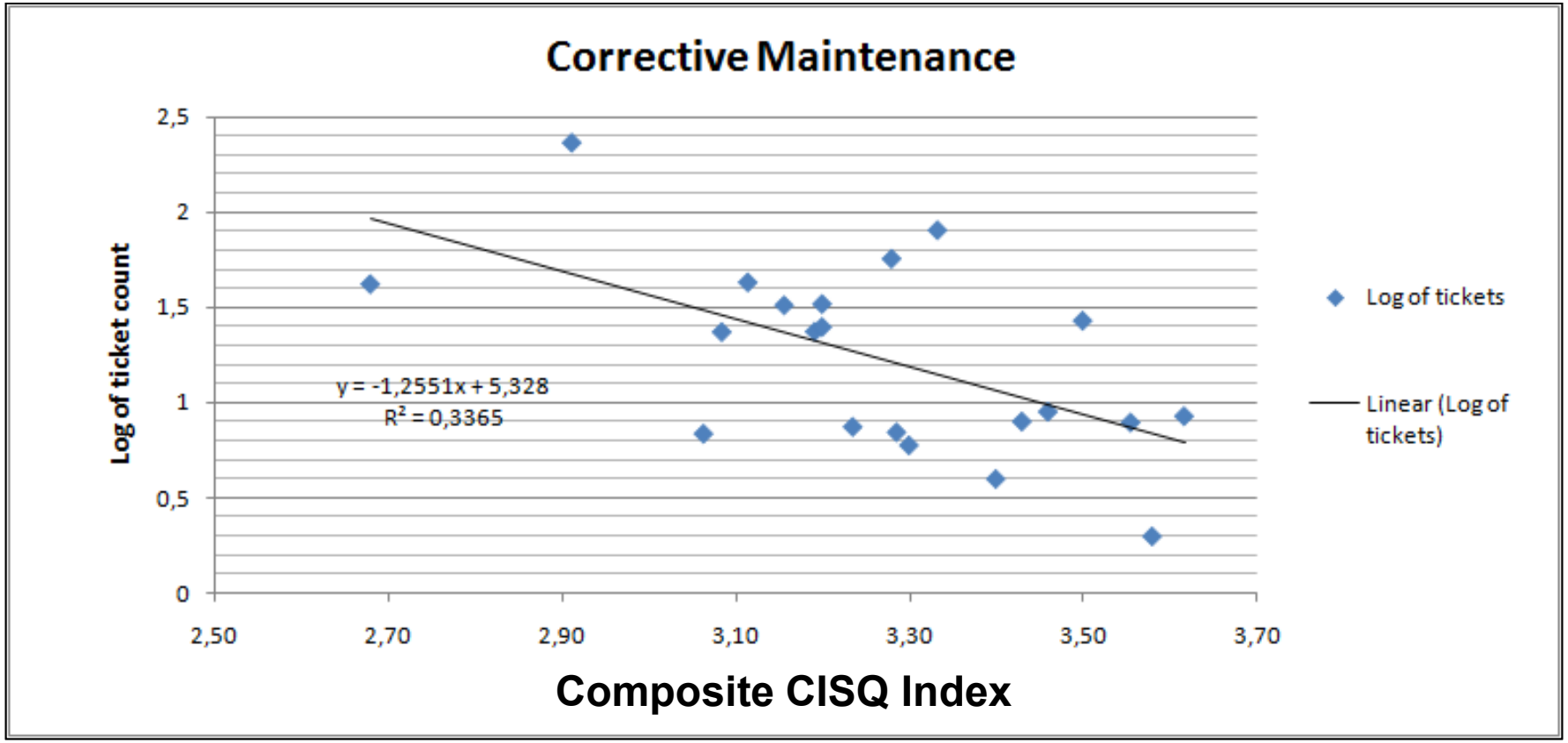


Jones, Capers. *Applied Software Measurement: Global Analysis of Productivity and Quality.*

© 2022 Consortium for Information and Software Quality (CISQ) www.it-cisq.org

Measures Predict Incidents & Costs

Study of structural quality measures and maintenance effort across 21 customer apps in a large global system integrator



An index increase of 24% decreased corrective maintenance effort by 50%

© 2022 Consortium for Information and Software Quality (CISQ) www.it-cisq.org

CISQ ISO 5055 For governance

Benchmarking and comparison:

In order to compare quality results among different applications, the Automated Source Code Quality Measures can be normalized by size to create a density measure (from the base measure).

ASCxM-density = ASCxM / AFP

where x = a software quality characteristic (R, S, PE, M)

Other weighting schemes

Weighting scheme	Potential uses
Weight each quality measure element by its severity	Measuring risk of quality problems such as data theft, outages, response degradation, etc.
Weight each quality measure element by its effort to fix	Measuring cost of ownership, estimating future corrective maintenance effort and costs
Weight each module or application component by its density of quality weaknesses	Prioritizing modules or application components for corrective maintenance or replacement

© 2022 Consortium for Information and Software Quality (CISQ) www.it-cisq.org

Typical SLAs for sourcing contracts

- **A large majority of the ADM contracts contain a structure where there is an "at risk" percentage cap, (e.g., 10%) of the monthly contract value with a weighting for each SLA.**
- **In most modern contracts, the weighting factor for software quality measures is typically "over weighted" at ~200%.**
- **The time period for collecting and reporting SLAs can vary by contract. New development is to analyze SLA compliance at the end of each bundle of defined activities, when performance of the entire work package can be measured.**
- **Most vendors will ask for 6 months of data before agreeing to an SLA. If you have that, and can produce it, few vendors will argue. Otherwise, most will negotiate a "burn in" period of 6 months.**

Name	Description	Type	Period	Baseline	Weight	Low	High	Annual Improvement
Security	The likelihood of potential security breaches of an application.	Unit	Monthly	0.02	35%	0.018	0.022	5%
		System	Monthly	0.02	35%	0.00	0.019	5%
Robustness	The risk of failure or defects that can result from changing an application.	Unit	Monthly	0.1	25%	0.09	0.11	5%
		System	Monthly	0.1	35%	0.07	0.10	5%
Performance Efficiency	How well the code handles unexpected events and how easily system performance can be reestablished.	Unit	Monthly	1	25%	0.9	1.1	2%
		System	Monthly	1	25%	0.8	1.0	2%
Maintainability	The difficulty and ease to maintain an application.	Unit						
		System						

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Guida tecnica all'uso di metriche per il software applicativo sviluppato per conto delle pubbliche amministrazioni

© 2022 Consortium for Information and Software Quality (CISQ) www.it-cisq.org

ISO 5055 & the Cybersecurity Framework

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

The 5055 Security measure (and others) can be used in numerous processes of the Cybersecurity Framework.

Empirical risk tolerance thresholds for software security

Contractual SLAs and audits for software security

Evaluation of software assets for security weaknesses

Continual improvement of software security

Periodic scans for software weaknesses

Software security and weakness data are shared

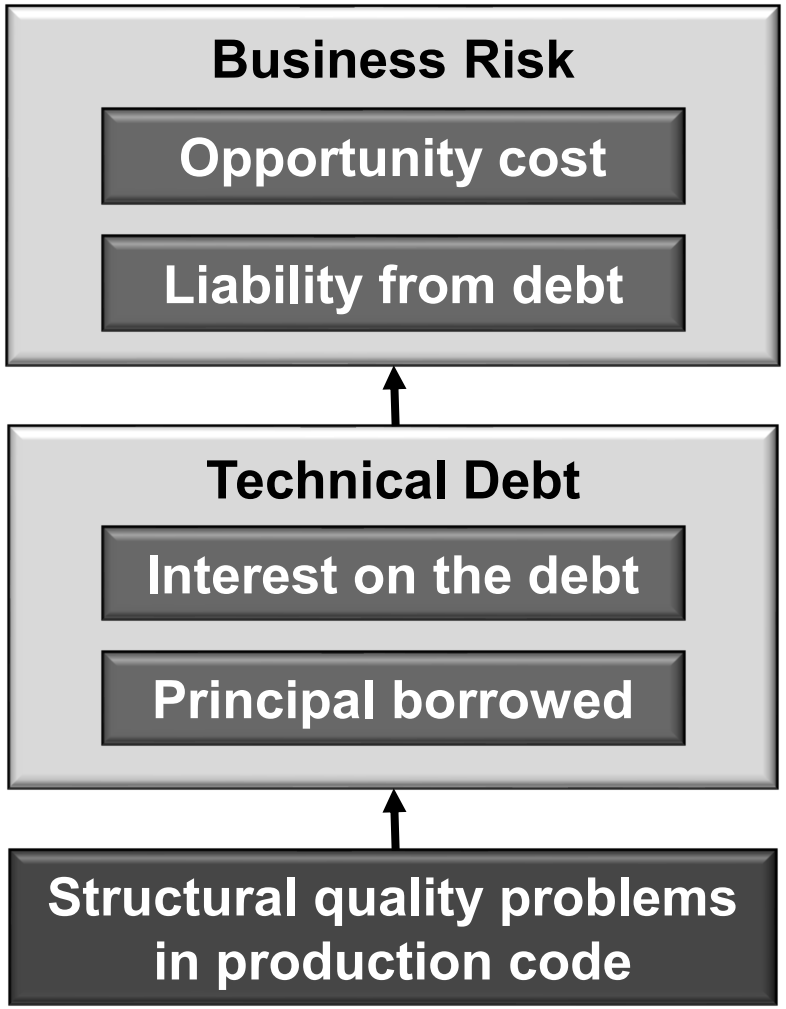
Security weaknesses are identified and mitigated

The 5055 structural quality measures play an important requirements and verification role for ‘Build Security In’ for cybersecurity

© 2022 Consortium for Information and Software Quality (CISQ) www.it-cisq.org

The Technical Debt Metaphor

Technical Debt — future costs attributable to flaws in operational code



Opportunity cost - benefits that could have been achieved had resources been put on new capability rather than retiring technical debt

Liability - business costs related to outages, breaches, corrupted data, etc.

Interest - continuing IT costs caused by the technical debt remaining in the code, i.e., higher maintenance effort, greater resource usage, etc.

Principal - cost of remediating must-fix problems remaining in the code

© 2022 Consortium for Information and Software Quality (CISQ) www.it-cisq.org

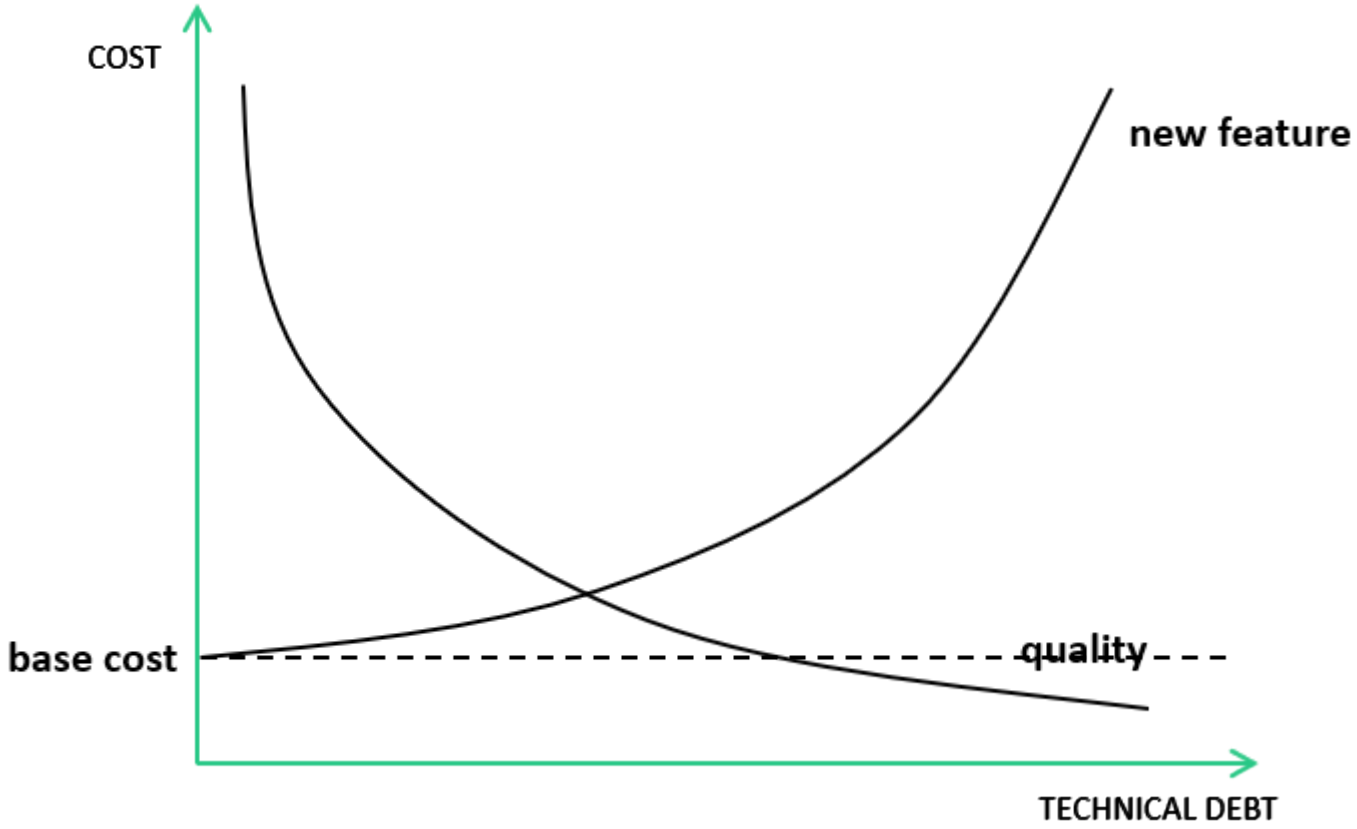
Curtis, et al. (2012)

13

Technical Debt dries up application value

Assumption: **Productivity is a stable number**

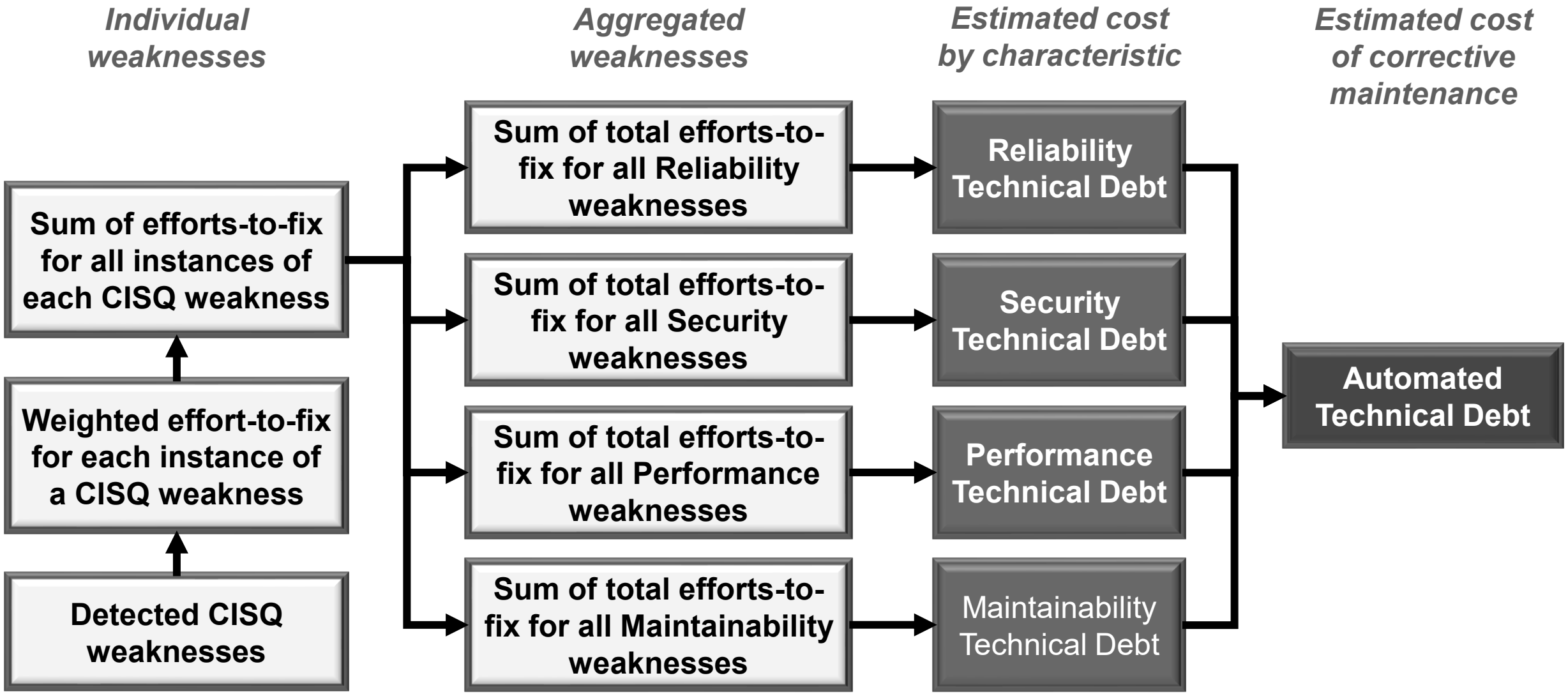
Reality: **Productivity is a monotonically decreasing function of releases**



Unless action is taken

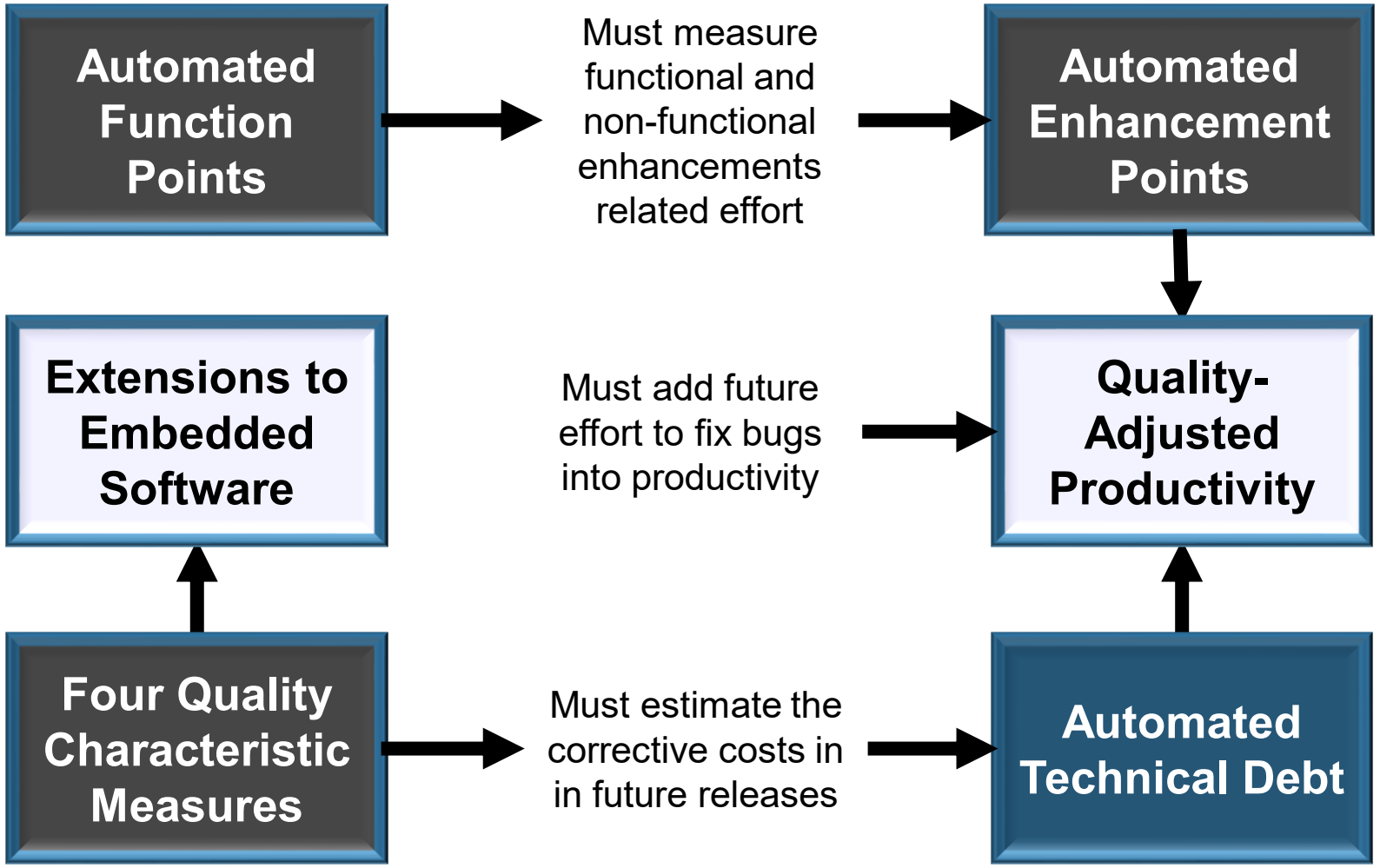
© 2022 Consortium for Information and Software Quality (CISQ) www.it-cisq.org

CISQ Technical Debt Measure



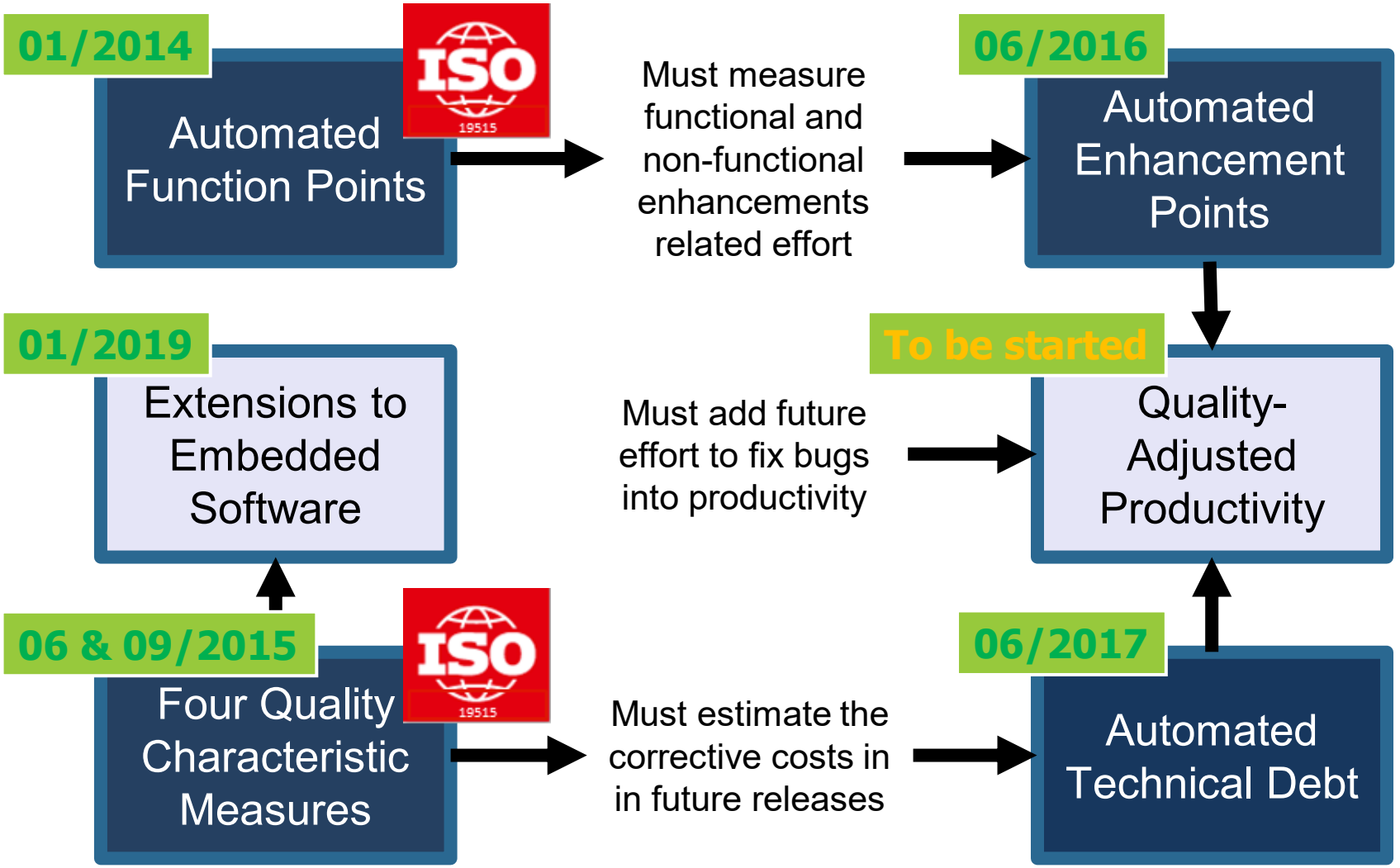
© 2022 Consortium for Information and Software Quality (CISQ) www.it-cisq.org

CISQ Measures Roadmap



© 2022 Consortium for Information and Software Quality (CISQ) www.it-cisq.org

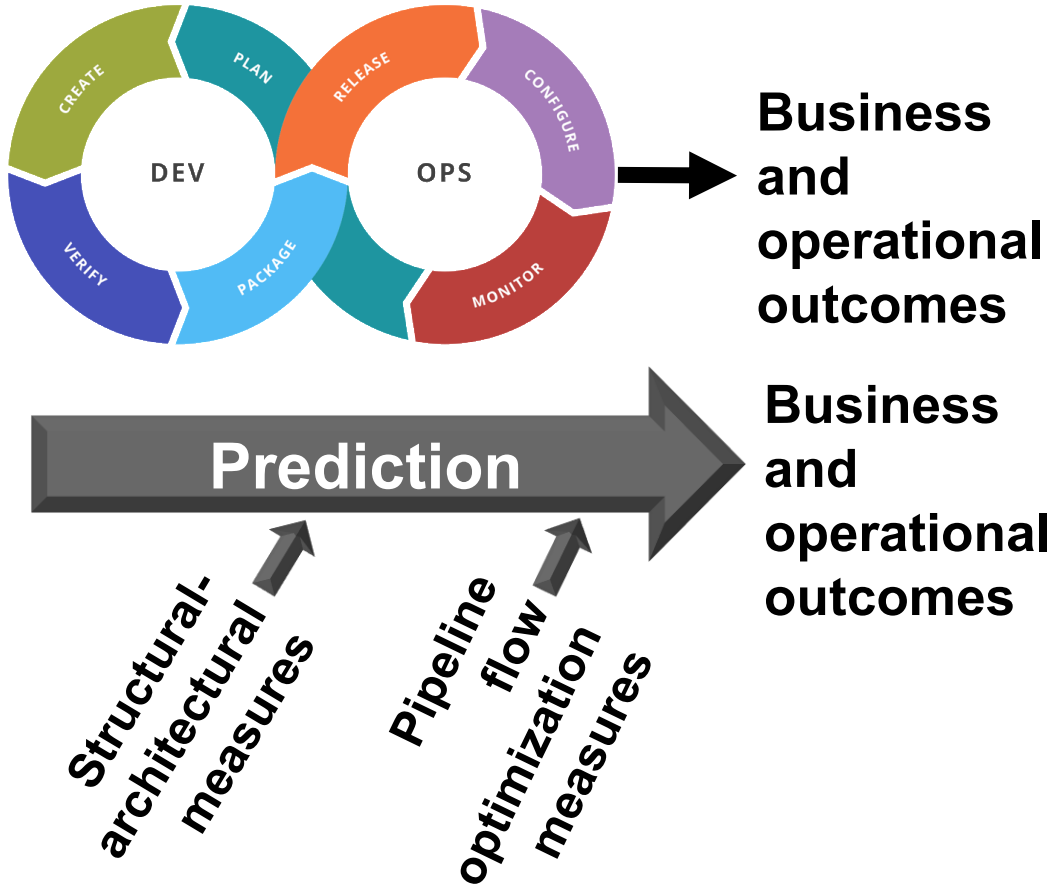
CISQ Measures Roadmap



© 2022 Consortium for Information and Software Quality (CISQ) www.it-cisq.org

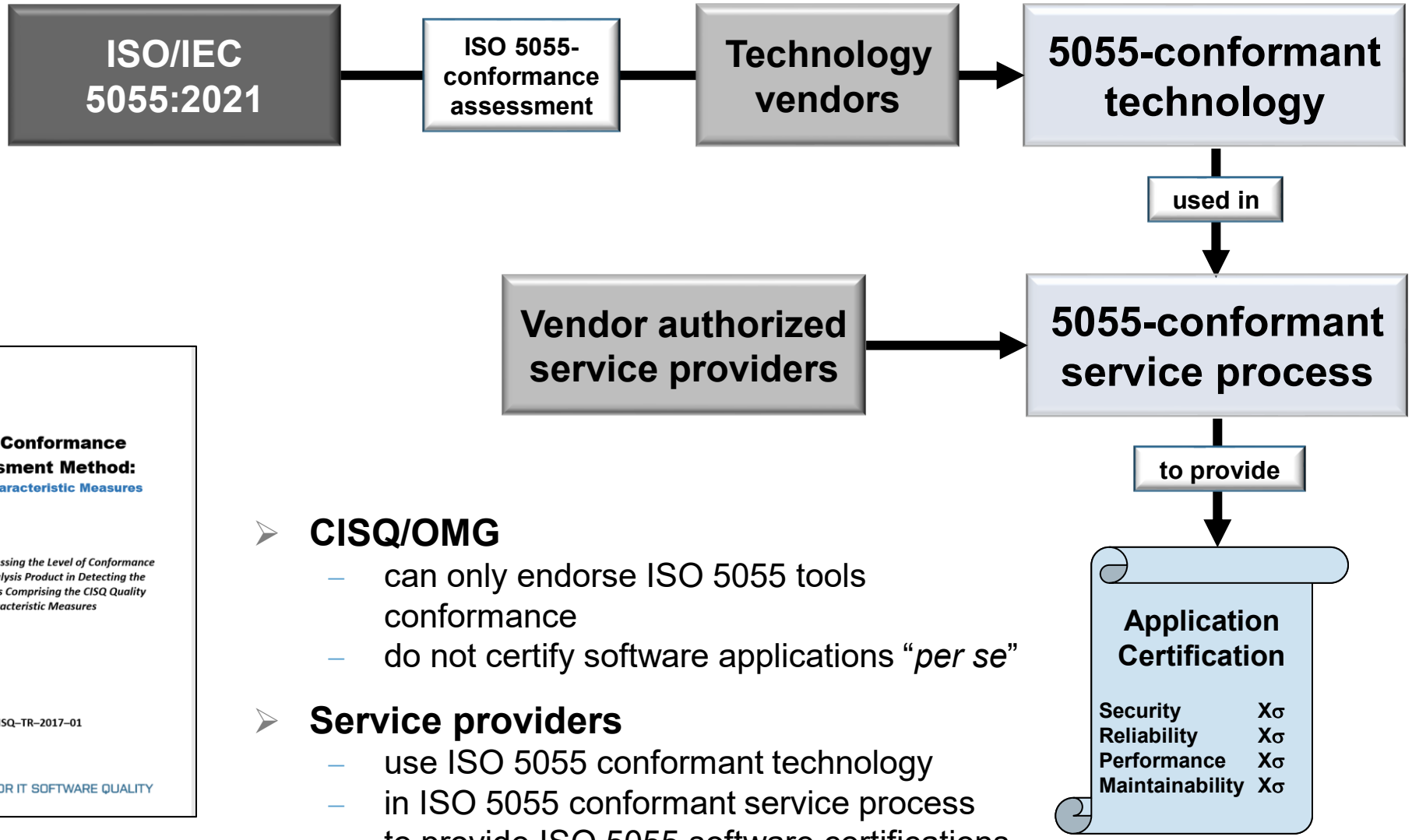
DevOps and Modernization Measures

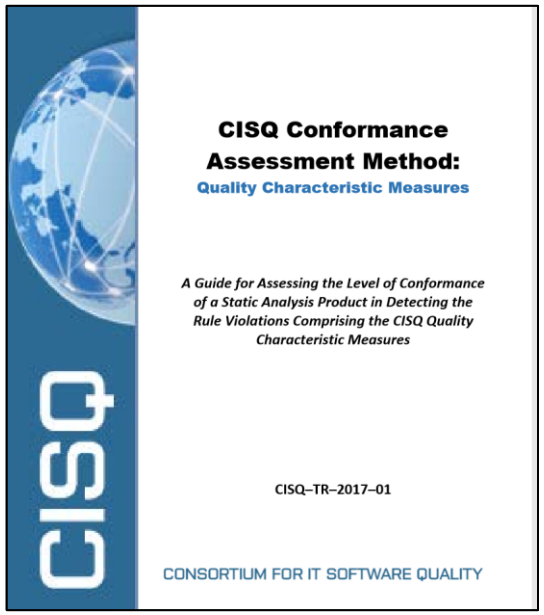
- **New project objective** – define standards for automatable Agile/DevOps measures
  - Prediction
  - Monitoring
  - Diagnostics
  - Benchmarking
- **Measures:**
  - DevOps flow and efficiency measures
  - Architectural modernization measures
  - Defect life measures
- **Project**
  - Inputs: Lean, PSM, CWEs, etc.
  - Output: OMG, ISO



© 2022 Consortium for Information and Software Quality (CISQ) www.it-cisq.org

Application Certification Using CISQ





- **CISQ/OMG**
  - can only endorse ISO 5055 tools conformance
  - do not certify software applications "*per se*"
- **Service providers**
  - use ISO 5055 conformant technology
  - in ISO 5055 conformant service process
  - to provide ISO 5055 software certifications

© 2022 Consortium for Information and Software Quality (CISQ) www.it-cisq.org

Green IT – Code sustainability

CISQ

Consortium for Information & Software Quality™

ABOUT CISQ STANDARDS EVENTS RESOURCES ACTIVE PROJECTS SPONSORSHIP

ASCRSM

HOME » ASCRSM

CISQ NEW STANDARD PROSPECTUS

AUTOMATED SOURCE CODE RESOURCE SUSTAINABILITY MEASURE

Motivation: Boards, shareholders, and regulators are increasing their demand for sustainable IT sol
sometimes called, 'Green IT.' Sustainable IT systems are conservative in their use of energy, hardwa
resources. However, the primary focus of sustainability is on minimizing use of energy and resource
environment. This is different from the earlier use of 'sustainable systems' to indicate systems that
scale so that they did not have to be replaced through expensive redevelopment.

The current effort is an evolution of a seminal work dating from 2014, codenamed "green-it" (and A
corresponding metric), and was a reference for practitioners and participants in the consortium u
experience, aiming to become defacto guidance in driving down energy waste across software im
evolved this preliminary specification into a robust standard measure.

Content: The specification for an Automated Source Code Resource Sustainability Measure (ASCRS
existing weaknesses (CWEs) in the Automated Source Code Performance Efficiency Measure (ASCPEM). Weaknesses that
affect resource usage from this standard will be supplemented with weaknesses from other ASCxM measures, as well as
relevant weaknesses not included in the ACSxM quality standards that affect resource usage. Only weaknesses that are
known to have substantial impact on resource usage will be included in the specification. The final specification is expected to
include 25-35 weaknesses. We anticipate any weaknesses not currently in the Common Weakness Enumeration Repository

CISQ has classified existing CWEs, pertaining to efficiency, reliability and system security, so to enable adopters to obtain:

- Classification of good vs, bad practices,
- Computation of a conformity ratio,
- Monitor of the trends and evolution
- Plan an improvement strategy

© 2022 Consortium for Information and Software Quality (CISQ) www.it-cisq.org

CISQ Membership Is Free — www.it-cisq.org

- **Almost 4000 individual members from Fortune 1000 organizations**
- **Contents:**
  - **Approved standards**
  - **Contract language**
  - **Trustworthy Systems Manifesto**
  - **Presentations**
  - **Webinars**
  - **Tutorials**
  - **Whitepapers**
  - **Use Cases**
  - **Blogs**
  - **News**
  - **Current standards projects**
  - **Process Maturity Metamodel**
  - **Upcoming events**
- **Cyber Resilience Summits**

© 2022 Consortium for Information and Software Quality (CISQ) www.it-cisq.org

Grazie per l’attenzione!

Contact:

michele.slocovich@it-cisq.org