CISQ

Consortium for IT Software Quality™

CISQ Standards for Federal Systems

Dr. Bill Curtis

Founding Executive Director, CISQ

Washington, DC

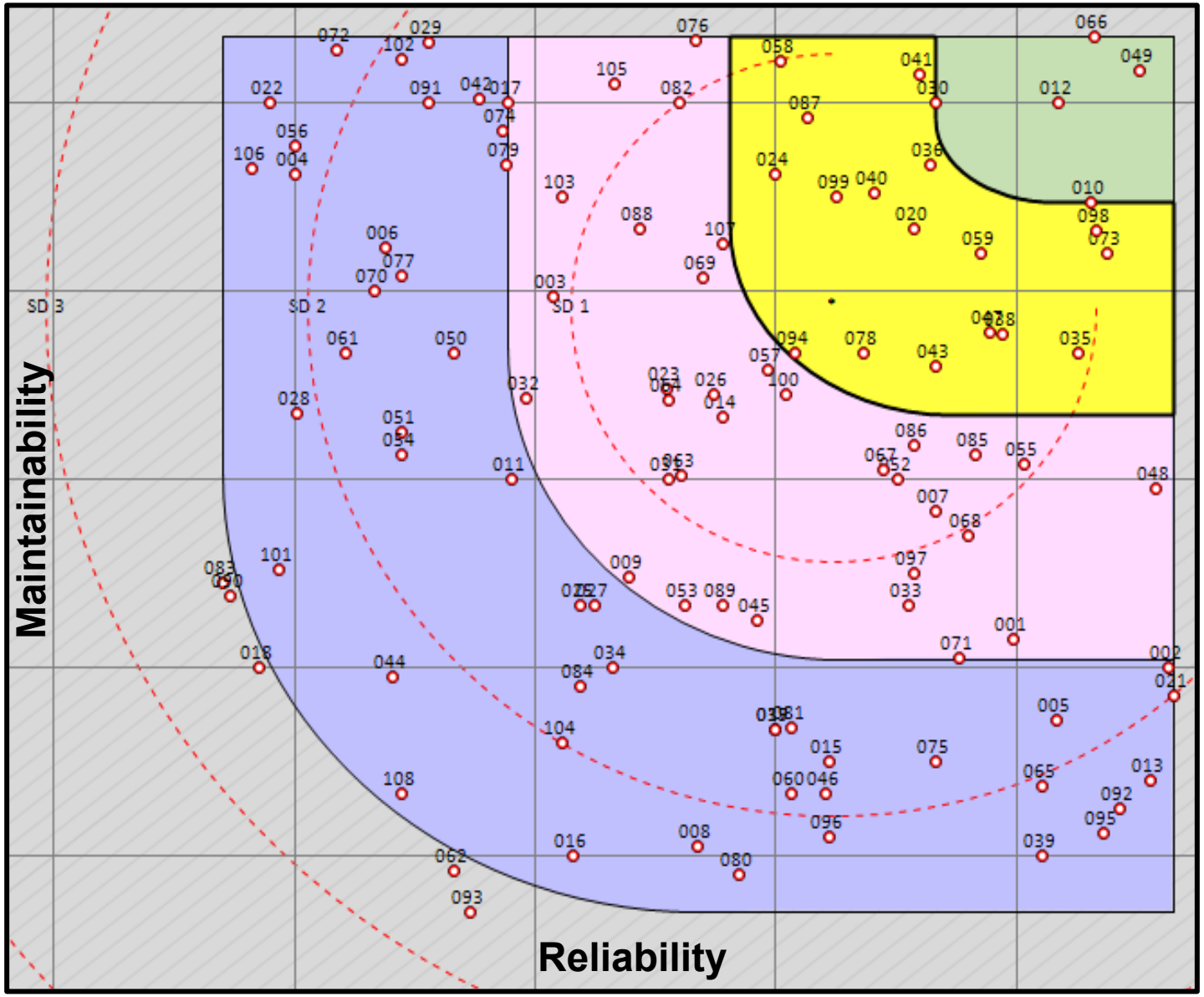
May 1, 2019

Why Do Software-Intensive System Projects Fail?

MITRE Study of Federal Systems

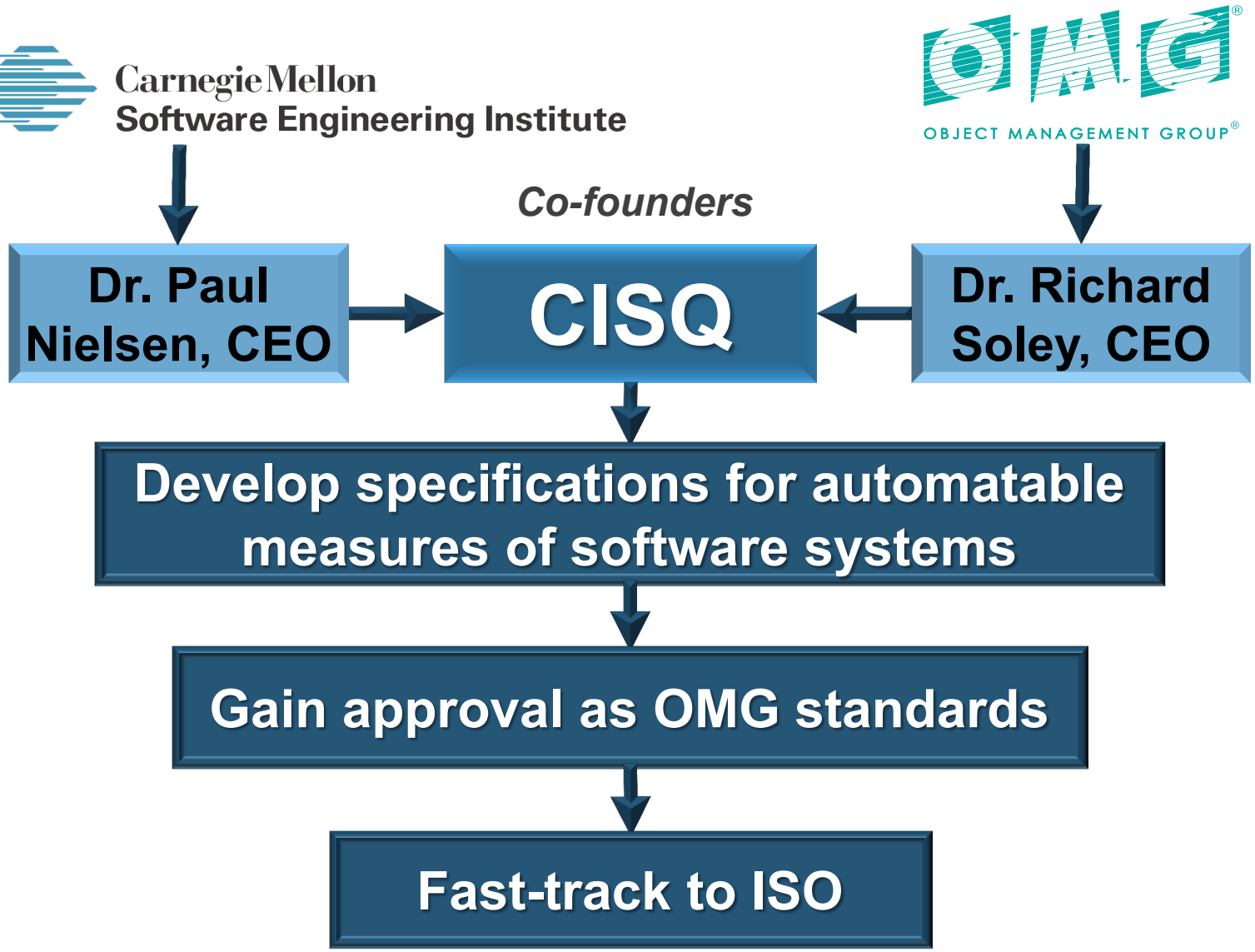
Software quality evaluation of 108 Federal systems regarding factors affecting operational and cost risk

Too high quality	**- 5**
Quality is good	**- 17**
Needs minor improvement	**- 34**
Needs major improvement	**- 46**
Outside range	**- 6**



John Marien, MITRE, 2019

What Is CISQ ?



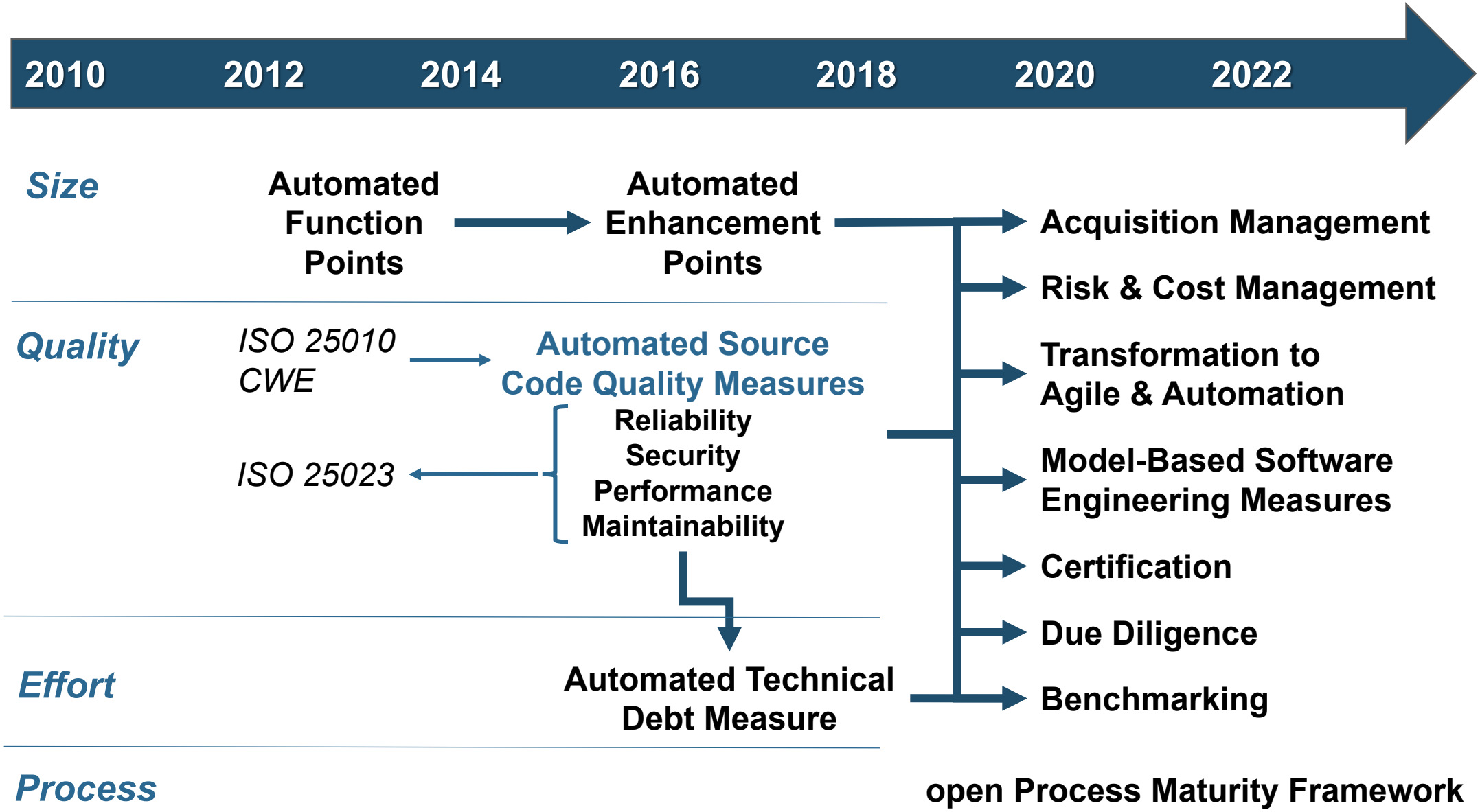
CISQ Sponsors

Cognizant
SYNOPSYS®
Tech Mahindra
SHPI
CAST
CGI
USC CSSE
NORTHROP GRUMMAN

CISQ Partners

Gartner
QuEST FORUM
FORRESTER®
IAOP
ITAAC
TECHWELL
AFCEA WASHINGTON, DC CHAPTER
MAKING SOFTWARE BETTER

CISQ Roadmap



CISQ and the NIST 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 CISQ Security measure (and others) can be used in numerous processes of the NIST Cybersecurity Framework. Some examples:

- **Empirical software security risk tolerance thresholds** ← ID.RA
- **Contractual SLAs and audits for software security** ← ID.SC
- **Evaluation of software assets for security weaknesses** ← PR.IP
- **Continual improvement of software security** ← PR.MA
- **Periodic scans for software weaknesses** ← DE.CM
- **Software security and weakness data are shared** ← RS.CO
- **Security weaknesses are identified and mitigated** ← RS.MI

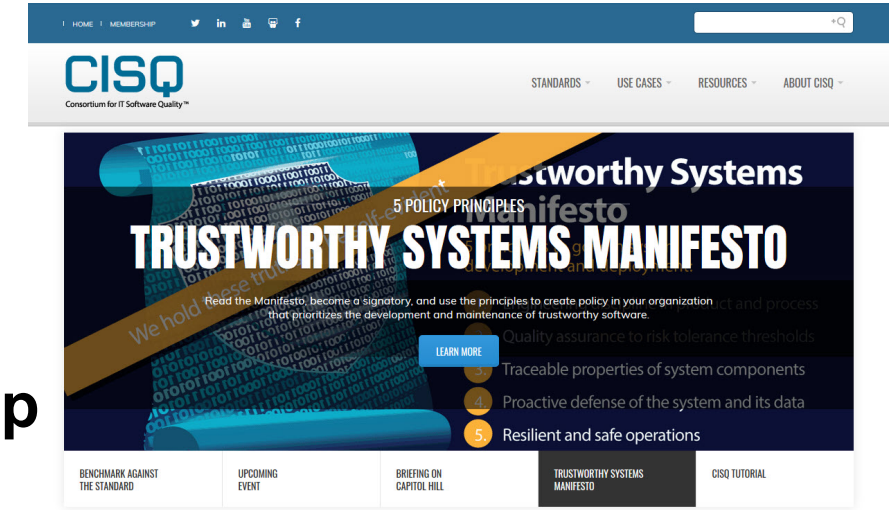
The CISQ structural quality measures play an important requirements and verification role for 'Build Security In' approaches to cybersecurity

Trustworthy Systems Manifesto

1. Engineering discipline in product and process
2. Quality assurance to risk tolerance thresholds
3. Traceable properties of system components
4. Proactive defense of the system and its data
5. Resilient and safe operations

www.it-cisq.org

Free membership



Summary

- CISQ measures provide industry standard quantification of software reliability, security, and cost risk
- CISQ measures are designed for automation and are supported by an ecosystem of vendors
- CISQ measures integrate seamlessly with modern agile processes, ISO standards, and NIST frameworks
- CISQ measures are already mandated in some government and industry acquisitions and can be written into policy