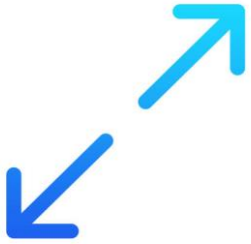
Measuring Data Privacy and Protection in Software
For CMMC, GDPR, CCPA, and HIPAA

Joe Jarzombek, Governing Board Member
Director for Government and Critical Infrastructure Programs, Synopsys

Cyber Resilience Summit 10/13/20

Introducing CISQ & Standards for Software Quality

CISQ is an IT leadership group that develops international OMG® standards for automating the measurement of software from the source code -



the **size** of a code base

for measuring development productivity

its **structural quality**

security, reliability, performance efficiency, maintainability

& **technical debt**

critical violations of good coding and architectural practice that live in the code

Leadership, Members and Partners

Dr. Bill Curtis
Executive Director

Joe Jarzombek
Governing Board Member

Co-founders:

OMG
OBJECT MANAGEMENT GROUP®

Software Engineering Institute
Carnegie Mellon University

Sponsors:

SYNOPSYS®
CAST
CGI
USC CSSE
Tech Mahindra
SHPI
NORTHROP GRUMMAN

Over 3,000 individual members from large SW-intensive organizations:

accenture
U.S. Department of Homeland Security
amazon
AXA
at&t
MITRE
Infosys
BOSCH
ISG
Capgemini
BOEING
aetna
Booz | Allen | Hamilton
CREDIT SUISSE
Capital One
IAOP
citi
Gartner
HCL
Atos
DUKE ENERGY
Allianz
DreamWorks
ca technologies
DELL
FedEx
Discovery Health
JOHN DEERE
DCG
CISCO
Fidelity INVESTMENTS
CenturyLink
IBM
BARCLAYS

Code Quality Standards

Security	Measures 74 CWEs in source code representing the most exploited security weaknesses in software including the CWE/Sans Institute Top 25 Most Dangerous Security Errors and OWASP Top 10
Reliability	Measures 74 CWEs in source code impacting the availability, fault tolerance, and recoverability of software
Performance Efficiency	Measures 18 CWEs in source code impacting response time and utilization of processor, memory, and other resources
Maintainability	Measures 29 CWEs in source code impacting the comprehensibility, changeability, testability, and scalability of software
Data Protection	Measures 89 CWEs in source code impacting data leakage or data corruption (potential vectors that could enable unauthorized reading or modification of data)

Use standards as requirements for delivering quality software free from critical vulnerabilities in code and architecture.

MITRE

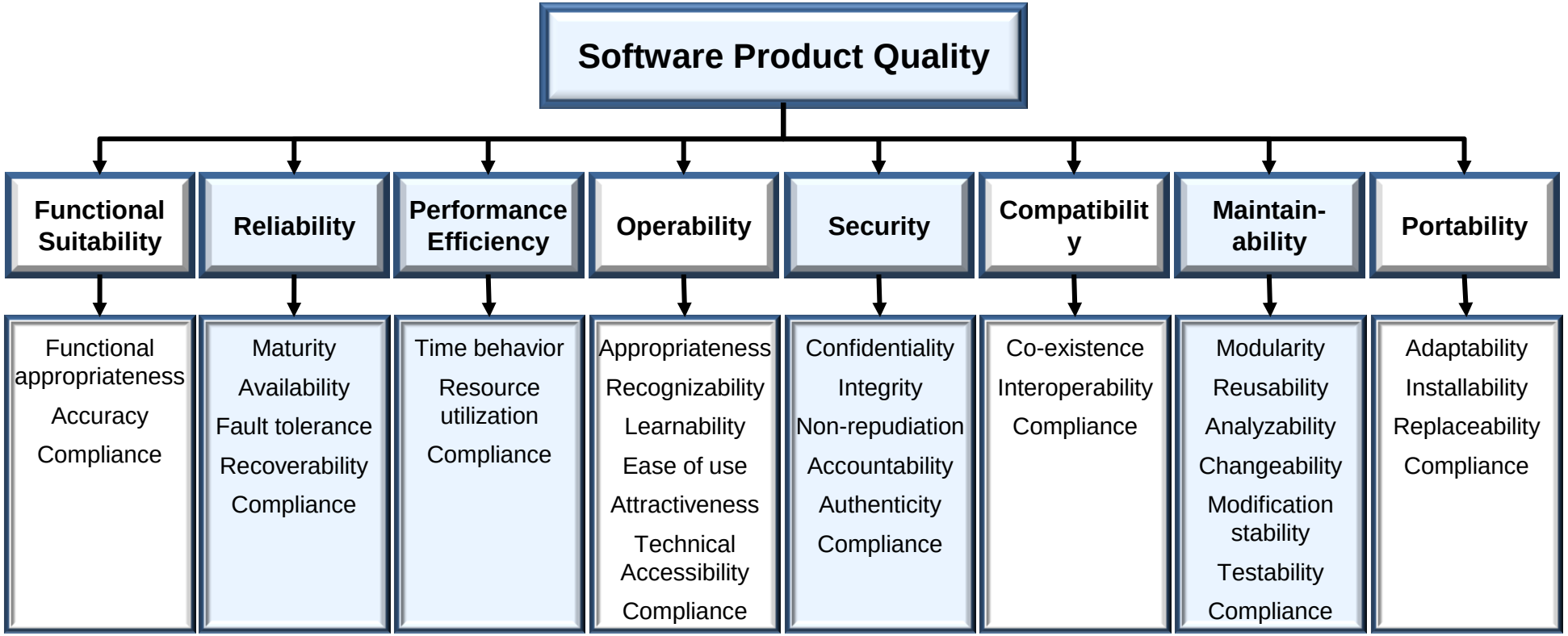
CWE Community

Standards available for free download at:

- www.omg.org/spec
- www.it-cisq.org/standards

Conforms to / Supplements ISO 25000 Series

- ISO 25000 series replaces ISO/IEC 9126 (Parts 1-4)
- ISO 25010 defines quality characteristics and sub-characteristics
- CISQ conforms to ISO 25010 quality characteristic definitions
- ISO 25023 defines measures, but not at the source code level
- CISQ supplements ISO 25023 with source code level measures



New Data Protection and Privacy Measure

- Supports enterprise and supply chain needs in protecting data, confidential information, IP, and privacy
- Contains CWEs associated with enabling data leakage – those that have CWSS technical impacts that enable unauthorized access to read/modify data
- Submitted in November 2020 to become OMG standard

Sampling of Data Protection CWEs

- CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer
- CWE-424 Improper Protection of Alternate Path
- CWE-595 Comparison of Object References Instead of Object Contents
- CWE- 597 Use of Wrong Operators in String Comparison
- CWE-667 Improper Locking
- CWE-764 Multiple Locks of a Critical Resource
- CWE-820 Missing Synchronization
- CWE-131 Incorrect Calculation of Buffer Size
- CWE-134 Use of Externally Controlled Format String
- CWE-704 Incorrect Type Conversion or Cast

Download full list of CWEs in the chat box
There are also architecture-level issues, not in code-level specification, but listed in informative table

Poll #1

Do you use these special pubs / standards?

__ NIST SP 800-171 Rev 2
__ NIST SP 800-53
__ ISO/IEC 27001

Data Protection and Privacy Regulations

Many organizations will be undergoing process assessments associated with CMMC for CUI, GDPR, CCPA, ISO 27001, NIST SP 800-53 r5, etc.

Scanning code that will run or is running in enterprise network-connected assets that process or transmit data would determine if the systems or devices enable data leakage or lack adequate protections to mitigate unauthorized access to read or modify data.

- If so, then such a scan would reveal if the data protection/privacy controls associated with the process assessment were inadequately implemented.

- Using the Automated Source Code Data Protection Measure would provide independent verification of processes revealing source vectors for data leakage or data corruption; providing indicators for non-compliance with respective Data Protection/Privacy guidelines.

MAPPING SOFTWARE-RELATED DATA PROTECTION CONTROLS in NIST SP 800-171 Rev 2, NIST SP 800-53, and ISO/IEC 27001

NIST SP 800-171 Rev 2 Security Requirements	NIST SP 800-53 Relevant Controls	ISO/IEC 27001 Relevant Controls
3.1 ACCESS CONTROL		
Basic Security Requirements		
3.1.1. Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems) 3.1.2. Limit systems access to the types of transactions and functions that authorized users are permitted to execute	AC-3 Access Enforcement	A.9.4.1. Information access restrictions A.9.4.5. Access control to program source code A.14.1.3. Protecting application services transactions A.18.1.3. Protection of records
	AC-17 Remote Access	A.14.1.2. Securing application services on public networks
Derived Security Requirements		
3.1.5. Employ the principle of least privilege, including for specific security functions and privileged accounts	AC-6 Least Privilege	A.9.4.5. Access control to program source code
3.1.7. Prevent non-privileged accounts or roles when accessing nonsecurity functions	AC-6(10) Least Privilege (prohibit non-privileged users from executing privileged functions)	*(no direct mapping)*
3.1.8. Limit unsuccessful logon attempts	AC-7 Unsuccessful Logon Attempts	A.9.4.2. Secure logon procedures
3.1.10. Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity	AC-11 Session Lock	A.11.2.8. Unattended user policy
3.4 CONFIGURATION MANAGEMENT		
Derived Security Requirements		
3.4.8. Apply deny-by-exception (blacklisting) policy or prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software	CM-7(4) Least Functionality *(Unauthorized Software / Blacklisting)* CM-7(5) Least Functionality *(Authorized Software / Whitelisting)*	*(no direct mapping)*

MAPPING SOFTWARE-RELATED DATA PROTECTION CONTROLS in NIST SP 800-171 Rev 2, NIST SP 800-53, and ISO/IEC 27001

3.5 IDENTIFICATION AND AUTHENTICATION		
Derived Security Requirements		
3.5.5. Prevent reuse of identifiers for a defined period	IA-4 Identifier Management	A.9.2.1. User registration & de-registration
3.5.6. Disable identifiers after a defined period of inactivity	IA-4 Identifier Management	A.9.2.1. User registration & de-registration
3.5.7. Enforce a minimum password complexity and change of characters when new passwords are created	IA-5(1) Authenticator Management (Password-Based Authentication)	*(no direct mapping)*
3.11 RISK ASSESSMENT		
Derived Security Requirements		
3.11.2. Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	RA-5 Vulnerability Scanning and RA-5(5) Vulnerability Scanning (Privileged Access)	A.12.6.1. Management of technical vulnerabilities
3.11.3. Remediate vulnerabilities in accordance with risk assessments	RA-5 Vulnerability Scanning	A.12.6.1. Management of technical vulnerabilities
3.12 SECURITY ASSESSMENT		
Basic Security Requirements		
3.12.1. Periodically assess the security controls in organizational systems to determine if the controls are effective in their application	CA-2 Security Assessments	A.14.2.8. System security testing

MAPPING SOFTWARE-RELATED DATA PROTECTION CONTROLS in NIST SP 800-171 Rev 2, NIST SP 800-53, and ISO/IEC 27001

3.13 SYSTEM AND COMMUNICATIONS PROTECTION		
Basic Security Requirements		
3.13.1. Monitor, control and protect communications (ie., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems	SC-7 Boundary Protection	A.14.1.3. Protecting application services transactions
3.13.2. Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security with organizational systems	SA-8 Security Engineering Principles	A.14.2.5. Secure system engineering principles
Derived Security Requirements		
3.13.4. Prevent unauthorized and unintended information transfer via shared system resources	SC-4 Information in Shared Resources	*(no direct mapping)*
3.13.8. Implement cryptographic mechanisms to prevent unauthorized disclosure of confidential unclassified information during transmission unless otherwise protected by alternative physical safeguards	SC-8 Transmission Confidentiality and Integrity	A.14.1.2. Securing application services on public networks A.14.1.3. Protecting application services transactions
3.13.13. Control and monitor the use of mobile code	SC-18 Mobile Code	*(no direct mapping)*
3.13.16. Protect the confidentiality of CUI at rest	SC-28 Protection of Information at Rest	A.8.2.3. Handling of Assets
3.14 SYSTEM AND INFORMATION SECURITY		
Basic Security Requirements		
3.14.1. Identify, report, and correct system flaws in a timely manner	SI-1 Flaw Remediation	A.12.6.1. Management of technical vulnerabilities A.16.1.3. Reporting information security weaknesses

Poll #2

Mark all applicable data protection and privacy regulations for which your organization might be interested in demonstrating conformance:

__CMMC,
__HIPAA,
__CCPA,
__GDPR,
__ other

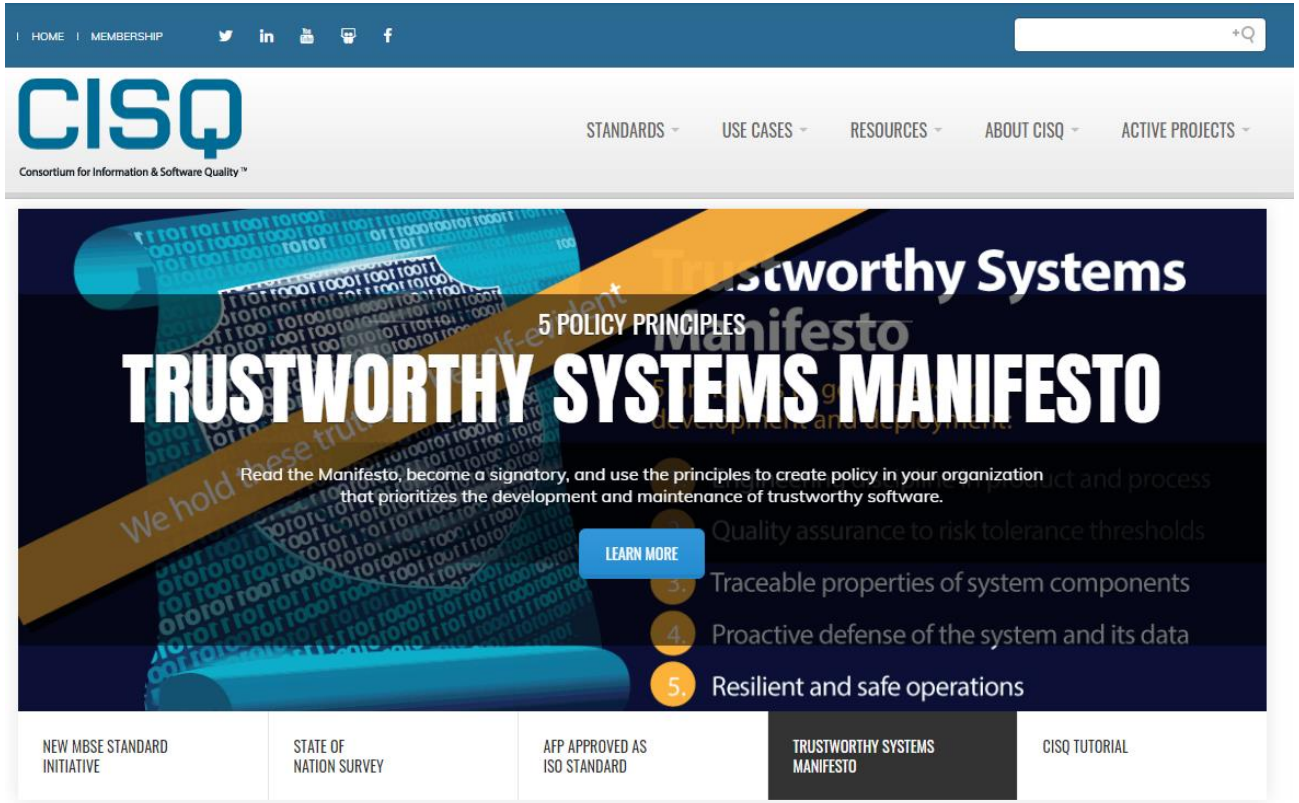
Conforms to / Supplements ISO 25000 Series

As follow-on effort, CISQ seeks to get this aligned with ISO/IEC 25000 series (25010 software product quality characteristics) to specify Data Protection as a sub-characteristic of Security.

Join CISQ, use the standards, contact us to learn more!

Dr. Bill Curtis
Executive Director
bill.curtis@it-cisq.org

Tracie Berardi
Program Director
tracie@omg.org



AUTOMATABLE STANDARDS FOR SOFTWARE MEASUREMENT

Send feedback on the Data Privacy and Protection Measure to info@it-cisq.org

www.it-cisq.org