Measuring the Cybersecurity and Resilience of Software Systems: ISO/IEC 5055:2021 Automated Source Code Quality Measures

Dr. Bill Curtis, Executive Director, Consortium for Information and Software Quality (CISQ)
curtis@it-cisq.org; 817-228-2994: PO Box 126079, Fort Worth, Texas 76126-0079

This submission jointly addresses items 3 (measures) and 4 (source code testing) in NIST's Call for Papers

While numerous standards address processes for producing and operating cybersecure and resilient software, until recently no international standards provided cybersecurity-related measures derived from analyzing a software system's source code. The recently published ISO/IEC 5055:2021 Automated Source Code Quality Measures fills this gap in cybersecurity measurement standards. ISO/IEC 5055 is a Publicly Available Standard originally developed by the Consortium for Information and Software Quality (CISQ, www.it-cisq.org), a Special Interest Group managed by the Object Management Group (OMG, www.omg.org) an IT standards organization. CISQ was co-founded by OMG and the Software Engineering Institute at Carnegie Mellon University.

ISO/IEC 5055 contains specifications for deriving measures of Security, Reliability, Performance Efficiency, and Maintainability from static analysis of the source code of software systems. These four measures are calculated from detecting and counting severe violations of good architectural and coding practices related to each quality characteristic that could result in unacceptable security vulnerabilities, operational risks, or sustainment costs. The team of international experts convened by CISQ from 24 organizations in North America, Europe, and Asia evaluated a wide range of software weaknesses and selected to include only those that were severe enough that they need to be eliminated from the code. Table 1 presents the number of weaknesses comprising each of the four measures with weakness examples.

Table 1. ISO/IEC 5055 Weakness Counts and Examples

Measure	Weaknesses	Example weaknesses
Security	73	SQL injection, Cross site scripting, Buffer overflows
Reliability	74	Improper synchronization, improper error handling
Performance Efficiency	18	Expensive loop operation, Unreleased memory
Maintainability	29	Excessive coupling, Layer skipping calls, Dead code

The four measures in ISO/IEC 5055 contain 138 unique weaknesses across the four measures, some of which are included in the calculations of two measures. For instance, buffer overflows can cause operational incidents (Reliability) as well as expose opportunities for hackers to gain unauthorized entry into systems (Security). MITRE has included all ISO/IEC 5055 weakness in the Common Weakness Enumeration Repository (cwe.mitre.org) and all are assigned CWE identification numbers.

ISO/IEC 5055 was developed in strict conformance to ISO/IEC 25010 which defines a product quality model for software-intensive systems. This model includes eight quality characteristics, four of which are quantified by the measures in ISO/IEC 5055. Each of ISO/IEC 25010's eight quality characteristics consists of several quality sub-characteristics that collectively define the domain of issues covered by

their parent quality characteristic. These sub-characteristics were used to ensure each of the ISO/IEC 5055 measures covers the range of issues in the domain of its quality characteristic.

ISO/IEC 25023 provides measures for the eight ISO/IEC 25010 quality characteristics. However, most of these measures only quantify the results of a software product's external behavior and do not measure weaknesses in the internal structure that cause these behaviors. ISO/IEC 5055 supplements ISO/IEC 25023 by providing measures derived from the internal structures of a product that affect its security, reliability, performance efficiency, and maintainability.

To aid static analysis vendors in automating the measures in ISO/IEC 5055, weaknesses are represented as one or more detection patterns formed from structural elements in the source code. Variations in how a weakness may be instantiated are represented by different detection patterns. These detection patterns are specified in the Knowledge Discovery Metamodel (ISO/IEC 19506) which characterizes the structural elements produced from parsing source code. The base measure for each quality characteristic is the total count of weaknesses detected for that characteristic. Derived measures of weakness density (weaknesses/size) or Sigma levels (weaknesses per million tested patterns) can be developed atop base measures.

ISO/IEC 5055 measures can be used for improving the cybersecurity and resilience of the nation's critical software-intensive systems and infrastructure in the following ways:

1. Existing software-intensive systems can be measured for the risk to which their cybersecurity and resilience weaknesses expose their mission or infrastructure. Evidence-based priorities for remediation can be established for the riskiest systems.
2. Standards for acceptable thresholds of cybersecurity and resilience can be set for software-intensive system acquisition. These thresholds can be written into Requests for Proposal, Statements of Work, and Contracts. Their achievement can be evaluated through static analysis during development and at acceptance testing. Thresholds can be established as targeted measurement levels to be achieved and/or weaknesses that are not allowed in the software. They can also be used in determining contract performance awards.
3. Automated estimates of the effort to eliminate weaknesses (a form of technical debt) can be established for the effort to fix each type of weakness adjusted by the complexity of the code in which it is embedded. OMG has approved a CISQ standard for this purpose. Such estimates are useful in allocating budgets for improving system and portfolio cybersecurity and resilience.
4. At each level of a software-intensive supply chain, software can be statically analyzed to identify unfixed ISO/IEC 5055 weaknesses. This information should be passed on either in a Software Bill of Materials, a management or configuration report, or other accessible form that ensures severe cybersecurity and resilience weaknesses are visible and transparent across the supply chain.
5. OMG is developing a certification for software developers to test their knowledge of weaknesses underlying the ISO/IEC 5055 measures. It will assess their knowledge of how to avoid, recognize, and correct these weaknesses. Results of this certification would indicate an individual's readiness to produce or sustain cybersecure and resilient software. The certification exam is expected to be available globally in 2022.

ISO/IEC 5055 is an internationally recognized standard that establishes a common basis of structural weaknesses incorporated into cybersecurity and resilience measures that satisfy part of the testing imperative (Section 4.r) in the President's executive order to improve the cybersecurity and resilience of the nation's critical software-intensive systems and infrastructure. ISO/IEC 5055 can be downloaded for free at: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html