CISQ Response to Enhanced Cyber Risk Management Standards

In response to Docket No. R-1550 and RIN 7100-AE-61

United States Federal Reserve System

Submitter: Dr. Bill Curtis, Executive Director (director@it-cisq.org)
On behalf of: Consortium for IT Software Quality (CISQ)
Regarding: Section V, Category 3 - Internal Dependency Management

CISQ (www.it-cisq.org) is a non-profit consortium managed by the Object Management Group (OMG.www.omg.org), an **IT** standards organization. CISQ is chartered to develop standards for automating the measurement of size and structural quality of software systems from their source code. CISQ has produced measurement specifications now approved as international standards by OMG for four quality characteristic measures (Reliability, Security, Performance Efficiency, and Maintainability) and two size measures (Automated Function Points and Automated Enhancement Points). OMG has begun submitting these standards through its fasttrack to ISO. CISQ offers the following comments and recommendations from its software standards activities as they apply to Section V, Category 3 - Internal Dependency Management. These comments and recommendations will be limited to the software components of a covered entity's internal cyber assets.

Question 17: While the proposed enhanced standards list "assessing the cyber risk of assets" and "continually applying controls and monitoring assets" (p.32), it does not provide additional detail on what practices would satisfy this portion of the enhanced standards. Most financial covered entities already implement quality assurance practices that could be argued to satisfy these two requirements of the proposed enhanced standards. However, in too many cases these practices are not sufficient to meet acceptable cyber risk thresholds. Specifically, the practices of covered entities are strongest for assessing functional quality (what the software is supposed to do), and weakest on non-functional or structural quality (how the software is constructed to do it). Most of the software-related IT outages and security breaches that make the news are the result of structural rather than functional flaws in the source code.

The enhanced standards need to enumerate the critical cyber assurance practices it would expect to observe were it to audit a covered entity. The assessment of software assets should include at a minimum; unit and integration testing, penetration testing, static analysis (especially focused on security and reliability weaknesses), processes for patching known vulnerabilities, dynamic program analysis, and load and stress testing under conditions that resemble those experienced in both normal and peak business operations.

Recommendation. The enhanced standards should consider including the CISQ Security and Reliability measures as either a recommendation or requirement for measuring the cyber risk of a covered entity's critical software system assets. These measures are based on an analysis of the extent to which a software system's source code is free from the most common and severe weaknesses that constitute software cyber risk. The CISQ measures provide a covered entity's Board of Directors with a testable means for expressing their risk appetite and tolerances for internal software assets. They can also be used as contractual thresholds for accepting software supplied by external vendors and third party service providers. IT management can present analysis of the CISQ measures as objective evidence regarding the extent to which critical software assets adhere to the Board's risk and tolerance thresholds.

The CISQ measurement standards were developed from known weaknesses in source code that can lead to reliability problems (outages, unexpected behavior, data corruption, etc.) or security breaches (unauthorized penetration, theft of data, malicious actions, etc.). They measure weaknesses that can occur at both the architectural (system) level, as well as in individual components of source code They should be applied both to internal application development and maintenance, as well as used in quality gates for accepting software from external providers. Covered entities should also require an evidence-based demonstration that Commercial Off The Shelf (COTS) software adheres to the covered entity's coding standards and cyber risk tolerances.

Security measure. The Common Weakness Enumeration (CWE) Repository maintained by MITRE Corporation with support from the Department of Homeland Security contains over 800 known weaknesses in software that hackers exploit to gain unauthorized entry into systems (Martin & Barnum). Every several years the software assurance community identifies which 25 of these weaknesses (CWEs) are the most dangerous and commonly exploited (aka the Sans Institute Top 25 and OWASP Top 10). The CISQ Security measure, available at http://www.omg.org/spec/ASCSM/, was developed from 22 the top 25 CWEs that can be detected through static analysis of the software.

Reliability measure. Although there was no industry agreement on the most severe reliability weaknesses, CISQ engaged 24 IT organizations, one third of which worked in the financial area, to develop a consensus list of reliability weaknesses. The 29 weaknesses identified became the CISQ Reliability measure, available at http://www.omg.org/spec/ASCRM/.

The measurement of cyber risk across an interconnected set of software applications constituting a supply chain that delivers a financial service is in the early stages of development. Supply chain cyber risk measurement is complicated since the interconnected software applications may be developed and operated by different organizations. At a minimum, measuring the Security and Reliability weaknesses in individual software systems will provide a basis for estimating the total supply chain vulnerability and cyber risk, as well as identifying weak links in the chain. The Agencies supporting the enhanced cyber risk standards should join with other Federal agencies and professional organizations to encourage and support the rapid development of software supply chain cyber risk measures.

Question 18: The initial cost burden of implementing enhanced cyber risk assurance practices will be offset by a near-term reduction in the cost of developing, maintaining, and operating internal software assets, as well as reduced liabilities from outages and breaches. Actions taken to reduce the cyber risk of software will enhance its overall quality. Research by Dr. Carol Woody who leads research on cyber security engineering in the Software Engineering Institute at Carnegie Mellon University has found strong correlations between the overall quality of a software system and its security, causing her lab to conclude that low quality software is insecure software (Ellison and Woody, 2010). In a similar vein, empirical software engineering research has consistently demonstrated that higher quality software is less expensive to maintain and enhance (Spinellis, 2006). Consequently, another near-term benefit of enhanced cyber risk practices is faster delivery of enhanced system functionality, resulting in greater business agility.

Experience in deploying the original Capability Maturity Model (CMM) burdened organizational software budgets with an additional 3% to 5%. However, these enhanced practices provided a return on investment averaging 5 to 1 as corrective maintenance costs, which averaged 40% or more in low maturity organizations, were typically reduced by half within 18 to 24 months (Hersleb, et al, 1997). The enhanced cyber risk standards would be expected to fit within this ROI profile since these practices will enhance the overall quality of software, thus at a minimum reducing corrective maintenance costs.

One of the challenges will be integrating enhanced cyber risk practices into an Agile Methods or DevOps environment. However, this is a process issue that involves integrating analysis and measurement tools into the integration, quality assurance, and release tool chains, and using the results to enforce release-to-production policies that are consistent with the enterprise's risk appetite. In most organizations, implementing the enhanced standards should be staged over a succession of applications rather than as a big-bang project. Lessons learned in initial implementations can be carried forward to successive implementations, thus shortening learning curves, improving outcomes, and easing the overall burden on the covered entity.

Question 19: Most covered entities have already implemented many common cyber risk assurance practices for their financially critical software assets. However, the breadth of practices and the discipline with which they are applied vary. The enhanced standards must be stated in terms sufficient for covered entities to discern the gap between their current practices and those of the enhanced standards. Many covered entities are currently using software security analysis tools to analyze their systems. A best practice adopted by many covered entities is to use several security analysis tools since the analytic approach and coverage of weaknesses varies across vendors.

Federal agencies could develop a joint program for training and certifying independent cyber risk auditors. Federally-certified, independent auditors with proven knowledge of quality assurance and cyber risk reduction practices can assess the rigor of implementations and the extent to which cyber risk practices are in standard use across internal assets. Compliance with the enhanced standards should be recertified at least every three years by independent auditors. Another option would be to allow private IT-auditing organizations such as the Information Systems Audit and Control Association (ISACA, www.isaca.org) who certify COBIT auditors to add the practices enumerated in the enhanced cyber risk standards into the audits they offer to covered entities.

Question 20: Federal agencies enforcing the enhanced cyber risk standards should require covered entities to prepare an evidence-based software assurance claim that their software and other covered assets and dependencies satisfy their Board's risk appetite and tolerances. OMG has developed a Structured Assurance Case Metamodel (http://www.omg.org/spec/SACM/) that provides guidance on the structure for developing a cyber risk assurance claim. The evidence supporting the claims could include results from various forms of testing, findings from independent internal audits, trends over incident logs, external process assessments against COBIT, ITIL, CMMI, or related frameworks, and other evidence relevant to cyber risk management.

The cyber risk assurance claim could be inspected by Federal agencies or independent auditors to ensure a covered entity complies with the enhanced cyber risk standards. In addition, the claim could be used as partial justification of the covered entity's cyber risk profile included in its quarterly financial reports, for assessing capital requirements under the Basel accords, and for demonstrating the Board's governance of its risk tolerances.

Questions 21 & 22: Covered entities are already requiring external suppliers to comply with various industry standards such as CMMI, ISO 9001, or the ISO/IEC 27000 series. Evidence of compliance is normally established through certified assessment results provided by independent assessors. In the case of CMMI this is not working well. Customers often complain about the quality of the software they receive from supposed 'CMMI Level 5' third parties because CMMI appraisals only assess the process and not the actual level of product quality.

The enhanced standards should be included as a supplement to existing standards used by covered entities for selecting and monitoring third parties. Covered entities should conduct their own due diligence assessments (often assisted by independent assessors) of third parties whose contract values exceed a Board-specified amount. Third parties should be required to present an evidence-based case that their processes meet required cyber risk standards and cyber risk tolerances as assessed by measures such as the CISQ Reliability and Security measures. In addition, vendors and third party service providers should be encouraged to adopt cyber risk measures for periodic monitoring of the extent to which their software activities are achieving the cyber risk tolerances and thresholds they are expected to meet in acceptance tests. The CISQ measures provide a common and precise language that can be used in third party contracts to specify customer expectations both in terms of cyber risk tolerance thresholds, as well as specific cyber risk weaknesses that may not exist in the source code at acceptance.

References

Ellison, Robert & Carol Woody (2010). Supply-Chain Risk Management: Incorporating Security into Software Development. *Proceedings of the 43rd Hawaii International Conference on System Sciences* (HICSS), January 5-8, 2010, Computer Society Press.

Herbsleb, James D., David Zubrow, Dennis Goldenson, William Hayes, & Mark Paulk (1997). Software quality and the Capability Maturity Model. *Communications of the ACM, 40,* 30-40.

Martin, Robert A., & Sean Barnum. *A Status Update: The Common Weaknesses Enumeration.* http://cwe.mitre.org/documents/cwe_update.pdf

Spionellis, Diomidis (2006). *Code Quality.* Boston, MA: Pearson.