Comments on Draft NISTIR 8170 – The Cybersecurity Framework
Implementation Guidance for Federal Agencies

Submitter: Dr. Bill Curtis, Executive Director (director@it-cisq.org)
On behalf of: Consortium for IT Software Quality (CISQ)
Regarding: Draft NISTIR 8170 – The Cybersecurity Framework: *Implementation Guidance for Federal Agencies*

CISQ

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. These comments primarily reflect the experience of CISQ's Executive Director from his 30 years of experience in improving the processes and measurement of software-intensive organizations, and his leadership of the team that developed the original Capability Maturity Model (CMM) in the Software Engineering Institute (SEI) at Carnegie Mellon University.

Overview

CISQ strongly supports the 8 uses of the Cybersecurity Framework as a desired end-state of a program to systematically reduce an organization's cybersecurity risk. The comments provided here are offered to improve the efficiency and completeness of achieving this end-state. The descriptions elaborating the 8 uses in subsequent sections generally take a top-down approach and focus on organizational level processes and actions. Other NIST documents supporting the Cybersecurity Framework have recommended a modified maturity framework to guide implementation. These comments will present modified implementation guidelines for NIST's consideration that blends top-down governance of risk with initial bottom-up implementation of risk reduction actions to ultimately create a strong organization-wide cybersecurity program. These recommendations are based on the original Process Maturity Framework that underlies the CMM and maturity models in other domains (workforce development, business process improvement) that have proven effective in numerous case studies of successful improvement programs. The recommendations are intended to offer one answer to the question, "How and in what order should our organization implement the elements of this guidance?"

Process Maturity Framework

As originally formulated by Watts Humphrey at the SEI, the Process Maturity Framework consisted of five levels, or stages of organizational maturity, that guided an evolutionary progression where each stage implemented increasingly sophisticated practices. Humphrey rejected the dominate top-down organizational improvement model of the day because he had seen failure rates as high as 70% in both software development and business process improvement programs. His unique insight was identifying a set of problems that needed to be eliminated in a staged order to enable continual and sustainable improvement. As the Process Maturity Framework has matured through years of implementation, its guidance can be reduced to 4 words: Stabilize—Standardize—Optimize—Innovate. A more complete description of these guidelines can be found in the member's area (free membership) of the CISQ website at http://it-cisq.org/wp-content/uploads/2017/05/Disputation-of-Misrepresented-Principles-Underlying-the-Process-Maturity-Framework-8-1-11.pdf.

Improvement programs that start by attempting to implement common organization-wide processes too often fail because standardized processes are pushed down on work units that are not sufficiently stable to adopt the processes successfully. For instance, work units that are understaffed will frequently fail to sustain processes directed from senior management because these processes are readily sacrificed in trying to meet unattainable objectives. It is this emphasis on initially stabilizing the cybersecurity practices of local work groups that motivates these comments.

Recommendations

The implementation guidelines in NISTIR 8170 describe an effort to create common organization-wide risk terms, cybersecurity requirements, cybersecurity processes, risk measures, reporting structures, etc. The descriptions generally imply the program is initiated at the organizational level by establishing these capabilities and passing them down to work units as cybersecurity requirements. The emphasis on a top-down approach is indicated by the predominance of senior management and administrative staff in the 'typical participants' for each of the 8 uses.

As a modification to this approach, the Process Maturity Framework would initiate the implementation program by combining the top-down governance responsibilities of senior management with a primary focus on having work units secure the systems, data, resources, practices, and other assets involved in their daily work. This provides and initial level of stability to the work unit's cybersecurity risk management. In these recommendations, a 'work unit' would be a team or other cohesive group assigned to work together on similar responsibilities, such as maintaining an application, operating a group of applications, managing data collection, interacting with citizens, or other functions.

To sustain improved cybersecurity practices, work units must establish control over the commitments for their work, the status and changes to their work products, the cybersecurity

practices most appropriate to their work, and the manner of handing-off their work products to other work units. The lessons from many successful organizational improvement programs guided by maturity framework principles suggest that initial cybersecurity requirements delivered by senior management should focus on these basic stabilizing factors before requiring broad standardization across the organization. The practices most consistent with these recommendations would be modifications of practices included in Use 5—Manage the Cybersecurity Program.

The role of senior management during this initial stage is to establish management's commitment to sustainable cybersecurity improvement, how this commitment will be enforced, the minimal requirements for complying with the first stage of improvement, and to ensure that the minimally necessary cybersecurity terms and practices are adopted as a starting point. This is similar to the CMM's guidance on establishing a minimally prescriptive life cycle process before beginning to elaborate detailed standard processes. The emphasis must be on the minimally necessary cybersecurity practices to stabilize and protect the cyber-sensitive assets in each work unit while meeting minimal regulatory requirements (HIPAA, FISMA, etc.). It is from this stabilization activity that each work unit can create a cybersecurity profile for the cyber-sensitive assets under its responsibility.

At the next stage, the organization can synthesize the most effective standard cybersecurity practices and measures from the various work unit profiles and integrates them into an end-to-end process flow across work units. Experience in developing standard processes and measures in other domains suggests that those who best know how risks can be minimized are usually those doing the work. The effort to standardize cybersecurity practices and measures should also incorporate and tailor specific practices described in other Cybersecurity Framework documents provided by NIST. Without work unit participation, organization-level groups who define standard practices usually overprescribe the process and fail to understand the necessary tailoring guidelines, guidelines that are best drawn from the daily experience of work units. Thus, experienced representatives from various functions should be included on teams defining standard cybersecurity processes and measures.

The advantage of this staged approach is to immediately focus on securing the organization's cyber-sensitive assets while preparing the inputs required to formulate a standardized cybersecurity framework with relevant tailoring guidelines. Since the standard cybersecurity framework is developed from inputs across the organization's work unit profiles, there is less friction when work units adopt standardized practices and measures. The measures required during the initial stage are those that help each work group identify, assess, and act on their cybersecurity risks. At the next stage, standards can be synthesized and enhanced from these unit-level cybersecurity measures that can be aggregated at the organizational level to assess enterprise and mission risk. For instance, basic component-level static scans of software for cybersecurity weaknesses conducted by developers at the initial stage can be supplemented by

more sophisticated system-level scans conducted during system integration as a standardized practice.

Once standardized cybersecurity processes, measures, and tailoring guidelines have been implemented, the organization can begin using the common measures and other cybersecurity information to evaluate their effectiveness, identify more granular processes and measures that would reduce cybersecurity risk, and establish organizational baselines and trends in critical cybersecurity risk items. If the organization needs further improvement it can use these data at the next stage to optimize the effectiveness of its cybersecurity practices and measures using advanced practices such as lean and statistical process control. If optimized processes do not meet the organization's risk tolerance objectives, it can experiment with innovative technologies, processes, training, and other mechanisms to reach it cybersecurity targets. The ultimate goal is to create an organizational infrastructure that is capable of meeting current cyber-risk objectives and reacting with necessary innovations to meet the cybersecurity challenges of the future.

Conclusion

CISQ recognizes that the NIST Cybersecurity Framework has adopted a non-prescriptive version of the Process Maturity Framework. These recommendations are provided as suggestions from past improvement program experience for accelerating the adoption and effectiveness of cybersecurity processes and measures. If these comments are helpful, CISQ is willing to assist in integrating them more closely with NIST's Cybersecurity Framework and implementation guidelines.