Comments on Draft (2nd) NISTIR 8286

Contributed by: Consortium for Information and Software Quality (CISQ)
Corresponding contributor: Dr. Bill Curtis, Executive Director, CISQ
Director@it-cisq.org

19 Enterprise risk created by the portfolio of software applications involves more than the issues typically associated with the term 'cybersecurity'. An example of a significant enterprise risk that is not security-related is the inability to innovate or response quickly to market changes because critical applications are so complex and sclerotic that implementing the needed enhancements is error-prone and uncompetitively slow. A title more inclusive of a wider range of risks such as 'Integrating Cyber Risks into Enterprise Risk Management' would be more representative. However, we recognize the issue that 'cybersecurity' is already woven throughout the fabric of the integrated document set.

572 Some standards that contribute measures useful for cyber risk already exist. CISQ and OMG have published a standard (https://www.omg.org/spec/ASCQM/1.0/PDF) for measuring the security, reliability, performance efficiency, and maintainability of a software system or application. These measures are built from measuring Common Weaknesses (CWEs) in a software application. MITRE has expanded the coverage of CWEs in the Common Weakness Enumeration (CWE) repository to include weaknesses beyond those associated with security, such as those associated with reliability or maintainability). CWEs are a recommended ITU standard. The CISQ software quality measures are "low level", foundational measures for measuring weaknesses that create operational risk or cost for a software application. These measures have been submitted to ISO for approval as an ISO standard that supplements ISO/IEC 25023 for software product quality measurement. This is the first critical step in establishing the enterprise risk contained in the critical software applications comprising an organization's IT portfolio. These measures are foundational in that they represent risks that can cause an application to suffer outages, response degradation, loss of confidential data, a skewing of cost toward corrective maintenance rather than new functionality, etc. NISTIR 8286 might consider referencing the OMG/CISQ measures as existing standards for assessing software risks at the product level.

802&9 A significant risk to the effectiveness of cybersecurity controls and mitigation actions is the knowledge, training, and experience of the officer(s) in charge of a risk or set of risks. Staff capability should be assessed since it is a major contributor to ERM risk management effectiveness.

This section would benefit from the inclusion of one or more examples of a hierarchical risk analysis model that:

1) aggregates low level risk factors, such as weaknesses in software that affect reliability,
2) into application level risk indicators,
3) that can be further weighted by context factors,
4) and might be further aggregated into an indicator representing the risk of a collection of interacting applications (such as an IOT system),
5) to correlate with operational problems, thereby identifying the probability of the risk's occurrence,
3) whose impact can then be quantified through analysis of the various costs of the factors impacted.

The subjective assignment of probabilities to the occurrence of a risk is a weakness in many ERM assessments. Exacerbating this problem is the dearth of data demonstrating the correlation between application risk measures and operational problems and costs. NISTIR 8286 should encourage both public and commercial enterprises to collect, analyze, and possibly even publish such data to establish a more objective basis for their risk occurrence probabilities. The subjectivity of these probabilities allows too much gaming of risk assessment outcomes.