Running Head: SSE-CMM

SSE-CMM: Moving up the Stack

Jered McClure

Walden University

SSE-CMM: Moving up the Stack

The Systems Security Engineering Capability Maturity Model (SSE-CMM) provides five architecture levels for defining systems security maturity. These levels are initial, repeatable, defined, managed, and optimizing. Assuring that each of these levels is met for a given domain should be a priority for any security project.

The “Initial” level is the beginning, where no policies and/or procedures have been put into place. This is the natural state of an organization prior to any security engineering. As such, this level has no assurances associated with it and is the level to most avoid. Essentially, being at this level means that the organization has applied no security to their system in question.

Being in the repeatable level means that an organization has a defined security policy and procedures for that policy. Furthermore, the policy and procedures are repeatable and followed for every project within the organization. A method of showing assurance at this level is through policy and procedural documentation. That is, for each project completed, documentation which checks off each relevant policy and procedure is supplied.

In the “Defined” level, policies and procedures are standardized throughout an organization. That is, each domain’s policies and procedures overlap other domains, thereby removing redundancy. Assurance at this level is gained through peer reviews, training programs, and intergroup coordination (Ferraiolo, 1998). Peer reviews provide a means for project members to voice their concerns about security and/or point out discrepancies in policy; training programs provide staff with the knowledge needed to understand security policies and procedures; finally, coordination between different groups assures policy is coherent between different security domains.

“Competence to manage various aspects of security engineering” defines the Managed level (Dhillon, 2007, p. 149). That is, security engineering is sustained at owner, system, and technical points. To gain assurance at this level, each of these points is accurately measured using predefined metrics. This ensures security excellence is maintained and measureable thereby “increasing awareness of shortcomings, pitfalls, and positive attributes of the process” (Dhillon, 2007, p. 149).

At the final level, Optimization, all the previous levels are upheld, additionally, improvement is sought for all security policies and procedures on a constant basis. This is done through a culture of change management, e.g. any policy or procedure alteration must pass through a change management body before being implemented. This safeguards the current status quo, while allowing the system security to adapt to changing environments when required. Assurance at this level is assessed through peer feedback and deterrence of security breaches, as well as, change management documentation.

This paper has defined assurance methods for each level of the SSE-CMM whereby an organization can gauge whether it has met a level of the staged CMM. The primary key at each point is a method of physically gathering evidence via documentation whereby proof is garnered that the level has been met and sustained. These assurances serve to provide a level of instruction for moving up the CMM stack without bypassing essential security requirements. In essence, no higher level is attainable in full until the previous level has been mastered.

Reference

Dhillon, G. (2007). *Principles of Information Systems Security: Text and Cases.* John Wiley & Sons, Inc.

Ferraiolo, K. (1998, October 7). *Tutorial: The Systems Security Engineering Capability Maturity Model.* Retrieved March 22, 2013, from National Institute of Standards and Technology: http://csrc.nist.gov/nissc/1998/proceedings/tutorB5.pdf