Capability Maturity and Appraisal Program

Student Name:

University

Professor Name:

Week2-Research Paper Topic

Abstract

Capability maturity essentially revolves around the appreciation of adequate information protection especially relating to sensitive and confidential aspects. Typically, capability maturity comprises a reference model that incorporates mature practices that are essential especially in the engineering discipline. Capability maturity and appraisal are essential tools for the organization to conduct an analysis of their security purposes of refining information confidentiality. It also offers customers a platform to evaluate and determine providers of security engineering service (Hefner, 2017). Capability maturity is a noble constituent and plays an integral role in facilitating security assurance advances.

The standard structure of the capability maturity and appraisal is formulated distinctly on the importance it has on information security assurance. The major objective of this topic is to determine the significances inputs of the maturity and appraisal program about information assurance and confidentiality (Hefner, 2017). Some of the common key component of this program includes; Specifying security requirement, operational security perils, verifying as well as validating security issues and availing security inputs. These components are key ingredients that organization considers making their preserved information safe and reliable.

Appraisals program basically provide information security that essentially defines the specified desired improvements and evaluate various deficiencies that an organization could be facing. Many organizations have embraced practice of engineering program for establishment of computer programs. This could be achieved through initiating operating system software's, middleware among other application programs (Stacey, 2017). It's, therefore, important to provide appropriate practices needed for a product developer, system integrator and aiding security specialist in identifying relevant information relation to security. With the wide

resilience of information among many societies, the absolute protection of such information has become vital across stake holder. This includes critical safeguard of classified and confidential government data, financial transaction, and personal information. The prevailing concerns of information protection have necessities the importance of security practices adoption.

The major purpose of evaluating capability maturity and the affiliated maturity appraisal is to have a candid comprehensive and have some distinct rationale thinking on its impacts on the information security insurance. Information security capability maturity encompasses five stages that provide insight and enlightenment on the prospected objectives in this course. Some of the crucial stages comprised in information security capability include; uncertainty, awakening, enlightens wisdom and benevolence. Uncertainty regarding capability maturity is described as a complete lack of comprehension concerning information security (Stacey, 2017). In this context, security is regarded as a paramount hindrance to productivity prospects. Although the integrity of the crucial requirement may be understood, failure to highlight reliability of information may result in failure in the security incidents. (Stacey, 2017)

Awakening which is the second phase in information security maturity is technically characterized by the realization of the absolute value of the information assurance as well as the time required to reinforce specified information security initiatives (Stacey, 2017). Information in this context is viewed accessible in the open market. Firm in this stage can procure system of choice especially those with high-reliability scale. Enlightenment features both the realization of detailed company information infrastructure and the resources required to support information security initiatives (Mellon, 2011). Enlightenment plays a crucial role in enabling the management to realize the essence of the information security in the overall and holistic structure of the entire enterprise. The wisdom which is classified as the fourth stage, evaluate the scope of

the information security and its reflection on the ideal environment for the diverse response associated to information. With increased comprehension in information security guidelines, management can effectively lay down well thought out information security policy (Mellon, 2011). Wisdom in this stage enables the management to establish informed decision that can be backed up with sufficient conviction for the sustainable purposes.

References

Hefner, H. (2017). *A Process Standard for System Security Engineering: Development Experiences and Pilot Results* (1st ed.). Retrieved from http://file:///C:/Users/admin/Downloads/Documents/A%20process%20standard%20for%20system%20security%20engineering%20development%20experiences%20and%20pilot%20results_p.pdf

Ferraiolo, K. (2017). *The The Systems Security Engineering Systems Security Engineering Capability Maturity Model Capability Maturity* (1st ed.). Retrieved from http://file:///C:/Users/admin/Downloads/Documents/916slide.pdf

Mellon, c. (2011). *Standard CMMI ® Appraisal Method for Process Improvement (SCAMPI SM) A, Version 1.3: Method Definition Document* (1st ed.). Retrieved from http://file:///C:/Users/admin/Downloads/Documents/11hb001.pdf

Stacey, T. (2017). *The Information Security Program Maturity Grid* (1st ed.). Retrieved from http://file:///C:/Users/admin/Downloads/Documents/82-10-40.pdf