Reflective Journal #3

Kenneth A. Piontek

Old Dominion University

CYSE 368 Internship

Dr. Saltuk B. Karahan

November 19, 2022

In this week's journal I'll be reflecting on another area of my job and a task that I worked on as it pertained to that domain. As an Information System Security Officer one of my primary responsibilities is the development, tracking, and management of POA&M's (Plan of Action and Milestones). A POA&M is one of the many parts of my job that are mandated by Federal Law, specifically the Federal Information Systems Management Act (FISMA) of 2002. A POA&M is a corrective action plan for tracking and planning the resolution of security weaknesses that are identified within an information system. These can be weaknesses that are identified throughout the course of a security assessment or identified by the ISSO throughout the course of managing one their other additional ancillary responsibilities. In creating the POA&M within the tool of record for C&A (Certification and Accreditation) management of our information systems first the root cause of the vulnerability needs to be determined by myself. I do this by working with the various stakeholders in order to confirm my understanding of the problem and with that determine the estimated cost and needed resources to complete the corrective actions that I want to institute. I then need to determine the severity level of the weakness. If this is something that I have identified as opposed to the deficiency being identified during an official assessment then using a risk matrix and or calculating the risk level using the CVSS (Common Vulnerability Scoring System) v3.1 calculator. The risk level assigned will then be the input I need for developing a timeline for remediation and also the measurable and identifiable actions that need to be done by the completion date. Hand and hand with this goes the monitoring of the weakness and keeping other stakeholders (primarily the system owner) aware as to prevent delays in scheduled completion dates.

One of the two information systems that I oversee is a cloud based system which was implemented as part of the federal government's cloud first initiative whereby a goal has been set

to move information systems into the cloud. This week I was focused on remediating findings for our most recent assessment performed by HQ. The system didn't receive a recommendation to or full authorization to operate. As such we've been put on a tight deadline in which a certain percentage of findings (percentage determined by severity) in order to get a reassessment of the system and then finally the authority to operate. The system is a critical one and is being built in parallel with the current future system of record, so to operate the other must be ready as well. There were two findings that took up the majority of my time. One of which was specifically pertaining to NIST 800-53 rev5 control RA-3 in which the information system is required to conduct a risk assessment and disseminate the risk assessment results to organization defined personnel. This was one of the easier to resolve and one that I'm able to write about. It involved writing the implementation for the control to accurately reflect the way in which the system is managed and as an artifact show the details of the recent assessment that was done. When first assessed it was a new system that had no such assessment so that was in turn a finding. With that assessment complete we were able to show the auditors at headquarters that we had an assessment in hand, that is reviewed on a daily basis and has been disseminated to all key personnel and the finding was closed out bringing us one step closer to having the authority to operate.