Internship Paper Four

Ashley Myers

CYSE 368 – 33455

Dr. Saltuk B. Karahan

July 1, 2023

Previously I had done a gap analysis on NIST 800-53 RA-3(3) Risk Assessment | Dynamic Threat Awareness. I was also assigned to do a gap analysis on CA-03(07) Transitive Information Exchange. We used Crysallis.AI to audit and perform this new assignment. I will attach the form along with this paper to give an outlook on what the organization was for this gap analysis.

NIST stands for National Institute of Standards and Technology. It is to help companies to have training on cybersecurity risk and to help reduce it. NIST 800-53 CA-03(07) section is Transitive Information Exchange. It is how systems exchange information between each other. Having the NIST is important because it guides and gives references to help set a standard plus some in the cybersecurity to help mitigate problems. While serving in the United States Navy my job used something like the NIST, but it was called NAMP, Navy Aviation Maintenance Program.

Everything maintenance action, had to be done by the book, and this was the book or in better terms publication to go by. This was the standards the Navy set and to make sure work got done correctly and to make sure one had a reference to what action they performed incase a mishap were to happen, they had themselves covered by following the directions. This is how I look at the NIST.

I got asked a question or more like a friendly pop quiz at work the other day where I brought up the NIST and that individual was impressed with me having this knowledge. The co-worker works in the cybersecurity sector of the company which made me look good for future job with the company. It is nice to have an internship no matter how big or small to hear or learn just a few things that could help one in the future in their career.

While performing my gap analysis with CA-03(07), I learned that this section talks about how one system talks to another, but before those exchanges there must be an approval for it to work. For an example, say a computer wants to use Microsoft outlook for their email system, there must be an approval and authentication for that company to use, and for the employees to log in.

Another example would be if one were to google search something on the web and come to a webpage that says access denied. This is telling the user that the companies IT and Cyber team does not allow access to webpages in that formality. There are interconnection agreements, information exchange security agreements, and service level agreements. When an individual gets hired and they must sign all the new paperwork, there is something that one signs to agree not to use the computers for wrongdoing and unauthorized usage. Now if an employee breaks that, they will be held liable and possibly fired for breaking that companies’ policy.

This section is important because it talks about how the interconnection are allowed, what devices should be allowed and helps employers get an idea and follow at least the standards that the NIST gives. If any company follows the NIST through and through, they should have no problem with security breaks or protocols within their company’s infrastructure.

References

National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations. *Security and Privacy Controlsfor Information Systems and Organizations*, *5*(3(7)). https://doi.org/10.6028/nist.sp.800-53r5