Journal Prompt from Module 1

Ray Montes Jr

25 May 2025

Ranking the top three categories for me would lead with my first choice being Oversight and Governance (OG). Without this, there would be confusion, chaos, no guidance, etc. For example, Cybersecurity Policy and Planning, Instruction, Compliance, and more all involve some steppingstones to create a path in which an organization can be competent and can become a well-organized and assembled unit.

Second would fall to Design and Development (DD) as this is a key role in any framework since you can either start from the ground up or use a general foundation that has been put out there for many to gain from. Upon creating or adapting a DD, reviewing Secure software Development, Systems Requirement Planning, Technology Research and Development, and more, they all require updates over time which is why DD is key for upper management and supervisors to always be thinking and finding new ways to make their products/teams better.

Third would have to be Protection and Defense since the world is evolving into an era where cyber threats are on the rise and the need for cybersecurity is vastly rising. This interests in the aspect of ensuring cybercriminals can’t access sensitive information from people since others might not know how to protect themselves.

Lastly, my least favorite would be Implementation and Operation, not in a bad way, but just because it sounds like the base level for most cyber related jobs. While it helps to know the basics and everything you do on a day-to-day basis, I just find this to be the grunt work and least appealing as compared to OG or DD.

References

Nice Workforce Framework for cybersecurity (NICE framework). National Initiative for Cybersecurity Careers and Studies. (2025, April 25). https://niccs.cisa.gov/workforce-development/nice-framework#:~:text=The%20NICE%20Framework%20is%20comprised%20of%20the%20following,required%20to%20perform%20tasks%20in%20a%20Work%20Role