

David Seliquini

CYSE 368

Summer 2026

Professor Teresa Duvall

TA Jade Hines

Wise Technical Innovations LLC

Reflection #2

Date: June 28, 2026

I have officially crossed the 100-hour mark of my cybersecurity internship at Wise Technical Innovations (WTI). While my first 50 hours were focused on building a baseline through the Certified CMMC Professional (CCP) boot camp, the bulk of these past 50 hours was spent tackling the next major hurdle: the 40-hour Certified CMMC Assessor (CCA) training course. Moving from the CCP to the CCA is honestly like moving from reading the rulebook to actually calling the game as a referee. This transition heavily supported my third learning objective, which focuses on executing practical compliance auditing.

The CCA course was a massive step up in complexity. In the CCP class, we focused heavily on understanding the 110 controls of NIST SP 800-171 and learning the basic vocabulary of the CMMC ecosystem. The CCA class, however, was entirely about execution and scoping. We spent a lot of time breaking down complex scoping scenarios to determine exactly where a company's secure boundary begins and ends. For example, we had to figure out how to classify Contractor Risk Managed Assets (CRMAs) versus

Security Protection Assets (SPAs) and determine how those classifications actually change the way a Certified Third-Party Assessment Organization (C3PAO) evaluates a network.

The most exciting part of these past 50 hours was diving deep into the CMMC Assessment Process (CAP). The training wasn't just theoretical; we worked through very specific, simulated client environments. We had to look at how different companies handle their objective evidence, like checking to see if their physical access logs match their digital access control matrices. Coming from a military background where procedural compliance is everything, this felt very familiar. In the shipyard, you don't just take someone's word that a valve is shut; you go physically look at the tag. The CCA course reinforced that exact same mentality for the digital world. You don't just assume a firewall is working because a client says it is; you check the configuration file and the interview logs.

The most challenging aspect of the CCA training was learning how to navigate the Shared Responsibility Matrix with External Service Providers (ESPs). Almost every defense contractor relies on cloud providers or managed IT groups these days, and figuring out exactly who is responsible for which security controls can get really messy. During one of the training scenarios, it was incredibly difficult to untangle whether the contractor or their cloud vendor was ultimately on the hook for a specific vulnerability management control. It takes a lot of patience to read through those service agreements and map them back to the NIST requirements without getting lost in the weeds.

Conclusion

Now that I have completed both the CCP and the CCA academic requirements, I feel incredibly well-equipped for the final stretch of my internship. With the heavy classroom lifting out of the way, my final 50 hours will be spent applying this assessor methodology during my regular Tuesday and Thursday shifts at the WTI office. I am looking forward to seeing how these scoping rules and assessment processes play out with actual clients, rather than just in training scenarios. Once I finish my last couple of office visits and hit the 150-hour requirement, I plan to shift my focus entirely to the final internship paper, where I will reflect on the management environment and the human element of auditing.