

Bridging the Gap: From Military Operational Compliance to Digital Risk Management

David Seliquini

August 9, 2026

Wise Technical Innovations LLC

CYSE 368: Internships in Cybersecurity

Summer 2026

Professor Teresa Duvall / TA Jade Hines

Table of Contents

1. Introduction.....	3
2. Management Environment.....	6
3. Major Work Duties and Assignments.....	9
4. Application of Cybersecurity Skills.....	12
5. ODU Curriculum Connections.....	15
6. Fulfillment of Learning Objectives.....	17
7. Motivating Aspects of the Internship.....	19
8. Discouraging Aspects of the Internship.....	21
9. Challenging Aspects of the Internship.....	22
10. Recommendations for Future Interns.....	24
11. Conclusion.....	25

1. Introduction

I decided to do my internship at Wise Technical Innovations (WTI) because it offered a very unique path into the world of federal compliance. When I first started looking for internships I was mostly looking at standard IT roles or offensive security positions. I applied to several different places using the ODU Monarch Internship and COOP portal but I kept coming back to the idea of doing something with risk management. As a transitioning Navy veteran with 14 years of experience in the Submarine Force and the Norfolk Naval Shipyard I realized I wanted something that would actually let me use my background in physical risk management and strict procedural compliance. WTI is a Certified Third-Party Assessment Organization (C3PAO). They specialize in helping defense contractors secure their networks and get ready for mandatory Department of Defense cyber audits. This seemed like a perfect fit for my skills.

The main reason I chose this specific internship over others was the opportunity to learn about the Cybersecurity Maturity Model Certification (CMMC). CMMC is the massive new standard that the government is rolling out to make sure civilian companies properly protect sensitive military data. The chance to actually get formal training on this framework was a huge selling point for me. I did not want an internship where I was just fetching coffee or resetting passwords all day. I wanted to do real work that would translate immediately into a civilian career. Knowing that WTI could provide me with the training hours needed for real world certifications made it the obvious choice.

When I set up my Memorandum of Agreement with Professor Duvall and my supervisor I had four very specific learning outcomes I wanted to hit. First I wanted to really master the CMMC ecosystem. I needed to understand exactly how the DoD the Cyber AB and the defense

contractors all work together. It is a very complex web of relationships and I wanted to understand who was responsible for what. Second I wanted to finish the educational training required to sit for the Certified CMMC Professional (CCP) exam. Getting that certification is a big deal in this industry and requires 50 hours of structured training.

Third I wanted to get real hands on experience with compliance auditing. I wanted to look at actual System Security Plans and see how companies try to follow the rules in the real world. I wanted to move past the theory and see the actual documents. Finally I wanted to prove to myself that my military operational discipline could translate directly into digital risk management. I wanted to see if the safety protocols I used in the shipyard were the same as the data protocols used by the DoD.

My initial orientation at WTI was definitely not a normal corporate onboarding. Most internships start with a few days of HR paperwork and watching basic training videos. Instead I was thrown right into the deep end. My first 50 hours consisted of an intensive boot camp for the CCP certification. My supervisor Koren M. Wise ran the class. It was a massive amount of information all at once. We covered everything from basic cyber hygiene to the complex scoping rules of the CMMC Assessment Process. We learned about the history of NIST SP 800-171 and why the government is pushing so hard for these new rules. It was a very intense way to start an internship but it set a really high standard for the rest of the summer and got me totally immersed in the work right from day one.

2. Management Environment

The management environment at WTI is very structured but also really open and collaborative. This makes a lot of sense when you think about what a C3PAO actually does. They are basically professional auditors so everything they do has to be perfectly documented and completely by the book. They cannot afford to cut corners or bend the rules because their own accreditation is on the line. The general management structure is pretty flat. My direct supervisor was Koren M. Wise and she is a CMMC Lead Assessor and Instructor. Because the whole business is built around following strict federal guidelines the supervision I got was very detailed and focused on specific objectives.

One thing that really stood out to me was how binary the management style is when it comes to the work itself. In a lot of regular IT jobs there are five different ways to solve a problem and they might all be okay depending on who you ask. At WTI it is very black and white. A contractor either meets the standard for a NIST SP 800-171 control or they do not meet it. There is no middle ground and there is no room for guessing. Coming from the military I really liked this style. I am very used to clear chains of command and strict procedural rules. Koren managed my workload by making sure I understood the regulatory framework first and then she let me practice applying those rules to fake network environments.

The leadership at WTI also puts a massive focus on continuous training and keeping up with the news. The CMMC program is still pretty new and the DoD changes the rules or puts out new guidance all the time. The management environment requires everyone to constantly read new policy updates to stay sharp. You cannot just learn the rules once and coast. You have to be actively reading the newest memos and federal register updates.

This need for constant awareness was super obvious when the recent 60 day suspension of the CMMC Phase Two rollout was announced a few weeks ago. When that suspension happened management did not try to hide the uncertainty from the team. Instead they were completely open about it. We had meetings where we discussed exactly how this delay was going to impact our daily operations and our clients.

Contractors were suddenly pausing their assessment plans because they wanted to wait and see what the government would do next. The way the management team handled this ambiguity and communicated the risks to the staff made me feel like a real part of the team instead of just a summer intern. It showed me what good leadership looks like in a crisis. They did not panic but they also did not pretend that the delay wasn't a big deal. They adjusted our training focus and kept everyone moving forward.

3. Major Work Duties and Assignments

My major work duties this summer were split into two very different phases. The first phase was all about academic certification training. The second phase was practical application in the office. For the first half of the summer my main assignment was completing 90 hours of formal classroom training. I did a 50 hour course for the Certified CMMC Professional (CCP) certification and then a 40 hour course for the Certified CMMC Assessor (CCA) certification. These assignments were completely necessary for the business. A C3PAO literally cannot operate unless its people are fully credentialed. By paying for my training WTI was investing in me so I could actually understand the documents I would be reviewing later.

The CCP training was all about building a foundation. We went through all the different domains of the CMMC model. We learned about the 14 different families of security controls in NIST SP 800-171. We spent days just learning the basic vocabulary. We had to know the exact difference between Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) because treating them differently is the whole point of the program. We also had to learn how to identify the different types of assets on a network. It was basically like learning a completely new language in a few weeks.

The CCA training was a massive step up in difficulty. This course was all about execution. We were not just learning what the rules were anymore. We were learning how to actually grade a company to see if they were following the rules. We spent a ton of time on scoping. Scoping is figuring out exactly where a company's secure boundary starts and ends. We had to figure out how to classify Contractor Risk Managed Assets versus Security Protection Assets. We also had to learn how to deal with External Service Providers like cloud vendors or managed IT groups.

In the second half of the internship my duties shifted to the actual WTI office on Tuesdays and Thursdays. My main project was helping the senior assessment team review sanitized client documentation. I had to read through massive System Security Plans and cross reference them against the 110 NIST controls. I was looking for objective evidence that a company was doing what they claimed they were doing.

For example one of the controls in the Access Control family requires companies to use multifactor authentication for all network access. My job was to review their access control matrices and interview logs to verify that MFA was actually turned on for every single remote connection. I could not just take their word for it. I had to find the hard proof in their configuration files. These duties are the core of WTI's business model. Without doing this deep evidence review the company cannot legally pass a defense contractor. If WTI passed a company that was not actually secure they could lose their C3PAO status entirely.

4. Application of Cybersecurity Skills

The cybersecurity skills I used during this internship were very different from what I expected. They were heavily focused on governance risk and compliance rather than technical hacking or network engineering. Before I started at WTI I had a pretty solid theoretical understanding of how networks work from my classes at ODU. I knew about firewalls and active directory and basic encryption. But I had to learn how to apply all those technical concepts to a very rigid set of federal regulations.

On the job I had to learn the specific scoping skills of the CMMC Assessment Process. I had to learn how to look at a complex network diagram and figure out which devices were actually touching sensitive data. You have to look at a network not just as a bunch of computers connected together but as a legal boundary that either protects data or creates a risk. I had to develop the skill of tracking data flow from an external email server all the way down to a specific user's laptop. This requires a lot of logical thinking and patience.

My time at the office completely changed my understanding of what cybersecurity really looks like in the corporate world. In school we spend a lot of time learning how to configure a firewall or how to run a vulnerability scan. In the real world I realized that a firewall is completely useless if the configuration is not documented and tested regularly. A vulnerability scan does not matter if there is no policy in place to actually patch the systems.

I also had to learn how to read a Shared Responsibility Matrix. This is a document that splits up the security chores between a defense contractor and their cloud provider. Reading those matrices was a totally new skill for me. If a contractor uses Microsoft GCC High for their email you have to figure out exactly which NIST controls Microsoft is handling and which

controls the contractor still has to manage themselves. You have to trace the line of responsibility very carefully.

This skill of mapping responsibility is incredibly important because a lot of companies just assume the cloud is perfectly safe. They don't realize they still have to manage their own passwords and endpoint protections. I now understand that technical skills have to be backed up by really strong documentation and policy enforcement or the whole security system will fail. You cannot have good security without good paperwork.

5. ODU Curriculum Connections

The ODU curriculum gave me a really strong baseline of technical knowledge but the internship definitely exposed a gap in my practical compliance training. Courses like CYSE 250 which covers basic cybersecurity programming and networking were super helpful. Because I took that class I understood how packets move and how subnets are designed. This was essential when I had to review client network diagrams at WTI. When a client talked about their VPN protocols or their endpoint detection tools I understood the underlying technology because of my university classes.

However the ODU curriculum did not really prepare me for the sheer volume of paperwork and regulatory mapping you have to do in the federal sector. I made a really strong connection between the concept of access control that we learned in school and the strict requirements of NIST SP 800-171. School taught me what access control is and why it is important. But the internship taught me how to actually prove to the government that a company is legally enforcing it.

There were several experiences at WTI that reinforced what I learned in school. For example in my classes we talked a lot about the principle of least privilege. At the internship I saw exactly how that principle is audited in the real world. We would look at user group policies to make sure that regular employees did not have local admin rights on their machines. It was cool to see a theoretical concept from a textbook being used as a hard pass or fail metric in a federal audit.

The internship also showed me a bunch of new concepts that I had not seen in school yet. The mechanics of a formal audit were totally new to me. Learning how to conduct an assessment interview without leading the witness was a huge learning curve. You have to know how to ask

open ended questions to see if the employee actually knows the security policy. Learning how to gather objective quality evidence without violating client confidentiality was also new.

Another new concept was the idea of Continuous Monitoring as defined by NIST SP 800-137. We don't spend a lot of time on that in school but at WTI it is a huge part of the job. You have to make sure the company isn't just secure on the day of the audit but that they have a plan to stay secure all year long. The ODU curriculum gave me all the technical vocabulary I needed but WTI taught me how to actually speak the language of compliance.

6. Fulfillment of Learning Objectives

When I started this internship I had four main learning objectives laid out in my Memorandum of Agreement and I am happy to say that I fulfilled all of them. My first goal was to master the CMMC ecosystem. I definitely achieved this through the intensive CCP and CCA training courses. I now have a really comprehensive understanding of the relationship between the Department of Defense the Cyber AB and the defense contractors. I know how the whole system is supposed to work from top to bottom.

My second goal was to complete the educational requirements to sit for the Certified CMMC Professional exam. I met this goal during the first few weeks of the summer. I completed the required 50 hours of sponsored training for the CCP and then I went above and beyond and completed the 40 hours for the CCA level as well. I now have the certificates of completion and I am fully eligible to sit for the official exams when I am ready.

My third objective was to get practical experience with compliance auditing. I fulfilled this during my regular office shifts on Tuesdays and Thursdays. By sitting with the senior assessors and reviewing actual System Security Plans I got real hands on experience. I learned how to trace objective evidence back to specific NIST controls. I learned how to identify gaps in a company's security posture that go way beyond simple technical flaws. I got to see how an auditing firm actually operates day to day.

Most importantly the internship fulfilled my fourth objective. I wanted to translate my Navy operational discipline into digital risk management. I successfully applied the strict procedural compliance mindset I developed in the shipyard to the digital boundaries of corporate networks. In the Navy you do not just trust that a valve is shut you go look at the physical tag.

At WTI I learned that you do not just trust that a firewall is working you go look at the configuration logs and the change management history. The internship proved to me that the strict safety protocols we used in the military are basically identical to the data protection protocols required by the DoD. The stakes are different but the methodology is exactly the same.

7. Motivating Aspects of the Internship

The most motivating aspect of this internship was realizing that my non traditional background is actually a massive asset in this field. When I first decided to transition out of the military and study cybersecurity I was pretty worried that my lack of deep IT experience was going to hold me back. I was worried that because I couldn't write complex python scripts I wouldn't be useful. But seeing how much of compliance auditing relies on discipline and procedural adherence was incredibly validating.

It was really exciting to sit in a conference room and look at a complex network diagram and realize that finding a vulnerability is just like finding a systemic flaw in a submarine tag out procedure. WTI gave me the chance to leverage 14 years of professional experience in a completely new industry. Every single time I successfully mapped a piece of evidence to a NIST control without needing help my confidence grew. It proved that I was on the right career path.

Another really motivating aspect was the mission itself. Knowing that the work WTI does directly impacts national security by securing the Defense Industrial Base gave the internship a real sense of purpose. I was not just pushing paper or filing reports. I was learning how to keep sensitive government data out of the hands of foreign adversaries.

Coming from the military that kind of mission focus is really important to me and it made coming to work every day very rewarding. I also found the people at WTI to be very motivating. They take their jobs very seriously but they are also very willing to teach. Whenever I had a question about a weird networking setup or a confusing policy document they would take the time to break it down for me.

8. Discouraging Aspects of the Internship

The most discouraging aspect of the internship was definitely dealing with the volatility of the federal regulatory environment. During the final few weeks of my time at WTI the DoD suddenly announced a 60 day suspension of the CMMC Phase Two rollout. Watching this delay impact the business was really frustrating.

It was discouraging to see defense contractors who were finally taking their cybersecurity seriously suddenly hit the brakes. They stopped their compliance efforts because the government changed the timeline at the last minute. It really highlighted how much of the cybersecurity industry is at the mercy of bureaucratic red tape. You can have the best security plan in the world but you are still waiting on politicians to make the final rules.

The delay also made the daily work a lot more difficult. The assessment team had to constantly manage client expectations without having any clear answers from the DoD. It was a stark reminder that even if you follow all the rules and do everything perfectly administrative delays can still totally disrupt your business operations. It was a good lesson in the realities of government contracting but it was still tough to watch.

Another slightly discouraging aspect was just the sheer amount of screen time required. Reading hundreds of pages of policy documents every day can be very draining. Sometimes it felt like I was reading the dictionary. It is not glamorous work. You have to really dig deep to find the motivation to keep reading when the documents are dry and repetitive.

9. Challenging Aspects of the Internship

The absolute most challenging aspect of the internship was the sheer volume of reading and memorization required to understand the NIST SP 800-171 framework. There are 110 different controls and each control has multiple assessment objectives that have to be met. Learning how to interpret the dense government style language of the CMMC Assessment Process was mentally exhausting. There were days during the boot camp where my brain just felt completely fried.

Furthermore applying those rigid rules to messy real world client environments was super difficult. It is one thing to know in theory that a company must have physical access logs. It is another thing entirely to look at a messy disorganized Excel spreadsheet provided by a client and try to determine if it meets the legal definition of an access log. You have to be incredibly detail oriented to spot the flaws.

Finally learning how to untangle Shared Responsibility Matrices with cloud providers was a major hurdle. Tracing the line of responsibility between a small defense contractor and a massive company like Microsoft requires extreme attention to detail. You have to read through pages of service agreements just to figure out who is supposed to be managing the encryption keys.

It takes a lot of patience to not get lost in the weeds. A lot of the time a client will think they are covered just because they bought a secure product. But you have to prove to them that buying the product isn't enough, they have to actually configure it correctly. Trying to explain that to a client without making them angry is a very difficult challenge.

10. Recommendations for Future Interns

My main recommendation for future interns at WTI or really any compliance focused internship is to familiarize yourself with NIST SP 800-171 before your first day. You definitely do not need to memorize the whole document but understanding its basic layout and the 14 families of security controls will save you hours of confusion. If you show up on day one knowing the difference between Access Control and Incident Response you will be way ahead of the curve.

Second I highly recommend brushing up on your technical writing and reading comprehension skills. This specific internship involves very little coding or network engineering but it involves massive amounts of policy review. Being able to read a 50 page corporate policy and quickly spot the missing security clauses is the most valuable skill you can possibly have in this job.

Finally future interns should prepare themselves for an environment where there is rarely a clear yes or no answer right away. You have to be comfortable operating in the gray areas of policy. You have to rely heavily on objective evidence to make a final determination.

You need to ask questions constantly and you cannot be afraid to admit when a client's documentation simply does not make sense to you. It is always better to ask for clarification from a senior assessor than to guess and pass a client who isn't actually secure.

11. Conclusion

To sum it all up my internship at Wise Technical Innovations was a completely transformative experience. It perfectly bridged the gap between my military career and my future in the civilian cybersecurity sector. The intense training I got in the CCP and CCA courses gave me a highly marketable skill set that goes way beyond what you can learn in a standard college classroom. I feel like I got years worth of industry knowledge crammed into one summer.

My biggest takeaway from this experience is that the cybersecurity industry desperately needs professionals who understand governance and risk management not just technical hacking. A secure network is built on verifiable policies and strict boundaries. These are concepts that I am now intimately familiar with thanks to WTI and the time I spent reviewing System Security Plans.

This internship will definitely influence the rest of my time at ODU. I plan to tailor all my remaining coursework to focus more on risk management policy development and systems auditing. I now have a very clear professional path forward.

When I graduate in the spring of 2027 I fully intend to leverage my Navy background and my new CMMC training to pursue a career as a federal compliance auditor. I want to help secure the Defense Industrial Base against digital threats and this internship gave me the exact tools I need to do that. Even with the current delays in the CMMC program I know this is the right field for me.