Alexander Berrios

Mr. Gregory Tomchick

Valor Cybersecurity

CYSE 368/Internship

Fall 2025

Final Paper

TABLE OF CONTENTS

Introduction…… 3

Leadership Environment……... 6

Work Duties & Projects……. 9

Cybersecurity Skills: Applied and Learned…… 10

ODU Curriculum Connections……. 13

Learning Objectives……... 17

Objective 1: Developing Security Solutions……. 17

Objective 2: Threat Analysis, Compliance, & Risk Management……. 18

Objective 3: CMMC Framework Familiarization…….. 18

Aspects of Interning at Valor…… 19

Most Exciting…….. 19

Most Discouraging……. 20

Recommendations for Future Interns…….. 21

Conclusion……... 22

Introduction

My internship at Valor Cybersecurity began from a mix of coincidence, determination, and necessity. Originally, I had a different internship arranged, but unexpectedly losing my job cost me that opportunity and forced me to scramble for an alternate one much later than I expected. I began searching for an opportunity to shadow a cybersecurity or computer science professional everywhere I could. I attended several job fairs, submitted applications online, reached out to school systems like Suffolk Public Schools and Norfolk Public Schools, city offices, local organizations, and any business that potentially had an IT department. Despite my effort, calls went unanswered, emails went unresponded to, and all communication was radio silent.

Out of desperation, I reached out to the internship coordinator at Old Dominion University, and by chance, she reviewed my resume and recommended reaching out to Valor Cybersecurity's CEO, Greg Tomchick. I contacted him immediately, we scheduled an interview, and after one conversation, he offered me an internship position. What started off as a stressful and uncertain search quickly turned around to be the most meaningful professional experience I've had. Even though I arrived at Valor unconventionally, everything aligned perfectly with my long-term goals.

I began my internship with four primary learning objectives. The first was developing scalable and adaptive security solutions, specifically through cloud computing services such as Microsoft Azure. My second objective was to strengthen my understanding of threat analysis, compliance, and risk management. My third objective was to familiarize myself with the Cybersecurity Maturity Model Certification (CMMC) framework, which outlines cybersecurity requirements for organizations with government contracts. My fourth objective was to learn how cybersecurity architecture integrates with business operations to see how documentation,

processes, client communication, and security strategies all align to support technical and organizational needs.

Valor Cybersecurity is a small cybersecurity business that was founded in 2021 by CEO Greg Tomchick. A prior player for the St. Louis Cardinals, he moved on to build a career in the cybersecurity industry. Valor specializes in cybersecurity compliance, security architecture, CMMC readiness, vulnerability management, and cybersecurity advising for organizations navigating cyber regulation requirements. Valor primarily works with defense contractors and small businesses that must comply with the Department of Defense (DoD) cybersecurity standards. The work at Valor requires balancing technical cybersecurity controls with small businesses and their operations.

Starting at Valor, I was introduced to the company's tools, workflow, and services. I was briefed on Valor's client portfolio, internal communication practices, documentation templates, and the overall outline of the organization. I spent my first days independently researching Microsoft Azure and reviewing CMMC requirements. Later, I was briefed on beginning a project plan for "ValorVictor", a secure, scalable software solution designed to streamline client documentation and other Valor services. Working on this introduced me to cybersecurity architecture fundamentals through familiarizing myself with Azure services and navigating elements of a secure portal, all while designing around CMMC compliance. I also began learning how Valor operates internally through Microsoft Teams, how we organize client materials and documentation, and how we structure projects to meet deadlines and compliance expectations.

My strongest initial impression of Valor was how collaborative the work is and how it contrasts with the independence granted to the employees, especially for a small business. Despite

the remote working environment, I felt included in the operations immediately. My early conversations with Mr. Tomchick and Jackson Walker, Valor's lead Cybersecurity Architect, made it clear that my internship was not going to be limited to shadowing colleagues through my computer or simply sitting in meetings to absorb information; instead, I'd be entrusted to actively contribute to client documentation, collaborating on security architecture designs, and helping with internal projects.

Jackson, who quickly became my primary mentor, shared his experience navigating the field, how he manages the workload of several clients, and his application of technical skills throughout his career. His guidance set the tone for the internship: independent, challenging, and rooted in creative problem-solving.

My first few weeks helped me transition from theoretical planning and research to hands-on practice, introducing me to areas of cybersecurity I had little to no experience in. By my second 50 hours, my responsibilities expanded to updating client documentation from CMMC Revision 2 to Revision 3, analyzing security plans, and learning how small changes in frameworks can significantly impact client security operations and risk management strategies

Overall, I am thrilled I was introduced to Valor Cybersecurity to complete my internship at. The beginning showed me that I would not only gain exposure to technical skills but also learn how cybersecurity can operate as a business service.

The management at Valor Cybersecurity is shaped by its identity as a small business operating in a highly technical field. Unlike larger organizations with strict chain of commands and departments, Valor's management is collaborative and adaptive. This environment allowed

me to not only work closely with leadership, allowing for direct exposure to executive-level decision-making, but also to experience hands-on operational work independently in a remote work environment.

Leadership Environment

Valor's leadership is shared between the CEO, Greg Tomchick, who oversees the company's direction, client relationships, and long-term growth, and Jackson Walker, a senior employee who has been taken under Mr. Tomchick's wing. As the founder and primary leader, Greg balances both business operations and cybersecurity strategy, shaping Valor's focus on ensuring client compliance. He leads Valor with Jackson Walker beside him after the departure of another team member early in my onboarding. Along with attending client briefs with Mr. Tomchick, Jackson became responsible for managing virtually all of Valor's clients, developing updated documentation, and standardizing fundamental internal processes. These roles helped give him a comprehensive understanding of the company's operations while simultaneously gaining leadership experience.

Because Valor is a small business, there are no layers of middle management; management is flexible and relies heavily on communication, trust, and initiative. This created an environment where my contributions were directly impactful; each "assignment" directly contributed to client readiness and ongoing security work.

Supervision was notably more mentor-driven than hierarchical. Greg and Jackson took a supportive and collaborative approach for guiding my work and consistently offered feedback. They periodically checked in on my progress and ensured I was set up for success with the

resources needed to succeed without being overbearing. Jackson, in particular, was a consistent mentor from the beginning. Although he works remotely, he still carved out time for regular phone and Teams calls, screen-sharing sessions, walkthroughs of CMMC documentation, cloud architecture development, and internal processes. However, his guidance went beyond technical skills; he shared meaningful career advice, efficiency practice tips, and advice on how to manage within a small-business environment. He described organization, time management, and efficiency as some of the most difficult but essential skills for cybersecurity professionals, especially when balancing high workloads and various deadlines

Supervision at Valor was also extremely flexible. Instead of micromanagement, I was trusted to conduct research, manage my workload, and pace myself independently. I was able to develop initiative, a deeper admiration of the work I was carrying out, and problem-solving skills, especially while working on unfamiliar tasks such as drafting documentation or analyzing CMMC Revision 3 changes. At the same time, leadership always remained accessible when I needed clarification or feedback, providing me an effective balance between independence and support.

Internal communication at Valor is primarily through Microsoft Teams, Outlook, and client-specific document folders via SharePoint. Because much of the company's work is remote, communication and clarity is essential. Early on, I was encouraged to maintain detailed notes, maintain organization, and document all updates or questions. This helped reinforce professional communication habits and ensured I was in sync with the team.

From my perspective, Valor's management environment is highly effective. The simple structure, mentored supervision, and collaborative work allowed me to experience a wide range of responsibilities that I wouldn't have been able to experience with a larger organization. I was able

to be exposed to architecture, compliance, documentation, cloud technologies, and risk management simultaneously. Not only did this accelerate my learning but it also helped me understand how cybersecurity functions within a business and as a business model.

Leadership's reliance on independent and initiative-driven employees also supported my learning objectives. To develop security solutions, understand compliance frameworks, and assist with carrying out business operations, I needed room to research and apply concepts independently. However, even with the independence I was granted, the accessible and supportive mentorship ensured I never felt lost or overwhelmed with my tasks.

Overall, the leadership environment at Valor is an ideal foundation for professional growth, autonomy, and exposure to real-world cybersecurity responsibilities. It challenged me to think critically, manage my time effectively, and take ownership of my learning, all while being supported by a team of professionals who were genuinely invested in my success.

Work Duties & Projects

My work at Valor Cybersecurity ended up being much more "hands-on" than I anticipated. From the beginning, I wasn't treated like someone who was just there to sit and observe. I was completing tasks that directly contributed to client documentation, internal projects, and long-term planning.

A significant portion of my internship involved helping update and maintain client documentation. This included System Security Plans (SSPs), Written Information Security Plans (WISPs), and Incident Response Plans (IRPs). Initially, the amount and length of paperwork were

extremely overwhelming, but slowly working through each document taught me how they fit together to build an organization's overall security posture.

Valor began transitioning clients from CMMC Revision 2 to Revision 3 during my second 50 hours, which pushed me to learn the updated requirements in detail. Updating existing materials meant reading line by line, identifying which controls changed, and figuring out how those changes affected a client's policies and operations. I was forced to slow down, maintain attention to detail, and understand how the documentation I was reviewing connected to real processes in a business.

My first major task involved learning the fundamentals of Microsoft Azure and helping plan the structure of a secure client portal project dubbed ValorVictor. During my first few weeks, most of my time was spent independently researching cloud architecture, Azure services, and how businesses utilize cloud platforms to build scalable and secure solutions. The goal of the ValorVictor project was to design a centralized portal where clients could store, access, and update their compliance materials efficiently and securely. My role wasn't to build the application from scratch, but to map out what the environment needed to look like and align those requirements with CMMC security controls. Not only did this help me familiarize myself with the technical designs and tools needed to create and sustain a secure cyber-architecture, it helped me learn how to translate an organization's needs into technical decisions that still meet compliance standards. This task helped me connect my academic knowledge and freelance research with real security design strategy.

Beyond documentation and cloud architecture planning, a lot of my tasks involved basic operational responsibilities: maintaining organized client folders, documenting changes, reviewing policies, checking revision dates, and cleaning up inconsistencies across files. These tasks taught

me the importance of structure and organization for cybersecurity. A single misplaced document or outdated policy could potentially delay an organizations compliance, cause confusion during an audit, or harm Valor's brand as a service-providing organization.

Upon reflection, my duties at Valor gave me a well-rounded experience that blended technical learning, compliance work, and hands-on support. Even though the work was time-consuming and at times challenging, it helped me grow into a professional who feels ready to take on more responsibility in the field.

Cybersecurity Skills: Applied & Learned

Before beginning at Valor, most of my cybersecurity experience came from classroom instruction, military service, and self-study. I had a decent grasp of networking fundamentals and basic security concepts, and a minimal understanding of cloud computing; however, one of the biggest areas of knowledge I strengthened throughout the internship was my foundational understanding of networking and security. Whenever I worked on documentation, such as SSPs or IRPs, I relied heavily on that knowledge to make sense of the technical environments clients were working with. Concepts like access control, network segmentation, authentication, encryption, and logging helped me interpret what controls applied to each client and why certain policies were written certain ways. Even though these concepts weren't new to me, seeing them applied in real organizational environments helped solidify my understanding and emphasized their significance to various organizations.

Regarding CMMC framework, I began from the bottom. I have heard of CMMC briefly through sites like LinkedIn, however, I didn't fully understand what it was or even how far

administrative structures could be intertwined with cybersecurity compliance. Beginning from the ground, I built up to my current level of knowledge and CMMC competence by working with the framework each day, learning how to interpret controls, identify gaps, and translating technical requirements into plain language that businesses could understand. A large part of this growth was through my exposure during Valor's client transitions from CMMC Revision 2 to Revision 3. During this period, I developed a deep understanding of the differences between the revisions, but the reasoning behind the updates and how those changes affected everything from documentation to risk management approaches. Through this, I was forced to think like a cybersecurity compliance analyst, not just a student taking notes or completing an assignment.

Cloud computing was yet another area where I gained knowledge. Early in the internship, I spent a lot of time learning Microsoft Azure fundamentals and understanding how cloud resources can support secure, scalable solutions for businesses. When I began helping with the ValorVictor planning phase, I had to combine what I learned about Azure with security controls from CMMC to design something that was both functional and compliant. Although my focus was realigned to dynamically support Valor operations and I was not able to get further than the planning phase, this experience helped me see that designing cloud architecture extends well beyond technology and into making deliberate choices that aligns with their respective regulatory requirements, protects data, and supports their unique business needs. Lastly, I learned how cloud services like identity management, network controls, and storage configurations play into the bigger security picture.

I also developed practical skills that don't always get emphasized in academia. Organization and documentation management skills turned out to be just as important as technical

knowledge. Maintaining organization was critical to maintain efficiency while working on multiple clients, navigating dozens of folders, reviewing policies, managing revisions, navigating through various tabs, all with only 2 monitors. You must know where everything is, what version you're working on, and how each document affects the final product. Jackson discussed this aspect of work often during the internship and emphasized that organization is one of the most difficult skills to master in the cybersecurity field because you're constantly learning new information while managing timelines and expectations. His approach to note-taking, standardized folder structures, and using tools to stay efficient helped me build these skills in a way that supported my work at Valor.

An unexpected area of growth came from learning how cybersecurity fits into a business context. Cybersecurity is usually presented as a technical field focused on defending systems and reducing vulnerabilities; however, at Valor, cybersecurity's administrative, strategic, and financial sides were emphasized in ways I was not exposed to during my undergraduate program.

Businesses have budgets, time constraints, personnel limitations, and operational realities that affect cybersecurity postures. Working directly with compliance documentation, client specifications, and even during my work designing ValorVictor, taught me that cybersecurity professionals must balance ideal security practices with what's realistic for a business. This understanding shifted my entire perspective, making my work and decision-making feel more dynamic.

Lastly, my perspective on threat analysis and risk management has shifted from a militarized and sometimes abstract approach to a concept that seems much more tangible to me. Spending hours reviewing documentation, identifying gaps, and revising policies allowed me to

see how risk plays a role in each part of an organization's cybersecurity strategy. Understanding where each business is vulnerable and how those vulnerabilities interact with compliance requirements helped me connect dots in ways I didn't see prior. I've become significantly more comfortable reading about threats, evaluating whether controls were adequate or needed, and understanding how certain weaknesses could impact the overall security posture of a company.

Overall, the internship helped me grow in multiple directions at once. I strengthened my foundational knowledge, gained exposure to technical frameworks, adapted to CMMC regulations, and developed a better understanding of how cybersecurity functions inside various organizations. The mix of technical work, compliance analysis, and operational responsibilities gave me a much more realistic picture of what cybersecurity looks like outside of coursework and helped me gain confidence in my abilities and knowledge.

ODU Curriculum Connections

A valuable part of this internship was discovering how much of the curriculum I learned at Old Dominion University connected to the real work happening at Valor Cybersecurity. Before the internship, I categorized my cybersecurity knowledge: security, networking, programming, Linux fundamentals, penetration testing, digital forensics, cyber law & policy, and so on. There were moments during my time as a Link 16 Network Designer or as a sailor that I could internally reference some of the things I was learning, but most of the time, it wasn't always clear how those subjects would come together in a job. My work at Valor was the first time I could actually witness how these pieces fit into a much larger picture.

Courses in networking, cybersecurity fundamentals, and techniques helped the most during my reviews of client documentation and interpreting security controls. During this work, I had to understand the various technologies clients were using and how those systems interacted with one another. Foundational security concepts like access control, multi-factor authentication, least privilege, encryption, and network segmentation were some of the first ideas I was exposed to in class and through labs. Identifying real-life applications of these controls reinforced their importance and helped me understand how different their implementation can look in various environments, depending on the client's size, budget, and operational needs.

Courses exploring cyber strategy, policy, and law, to my surprise, were much more relevant than I initially expected. My first introduction to NIST standards, risk assessments, and documentation requirements, I viewed them as paperwork that simply outlined and defined cybersecurity. I paralleled them to regulations or similar documentation I was exposed to in the military; these were regulations and references I could refer back to when needed, not something I'd need to analyze intensely or read front-to-back.

At Valor, compliance, regulation, and framework became the backbone of nearly everything I did. The transition from NIST SP 800-171 Rev. 2 to Rev. 3 required me to familiarize myself with all the documentation Valor was concerned with before supporting the transition effort; learn the resource names, understand what they're written for, understand their differences, and how they play upon one another. There was no way I'd be able to support Valor's team of CMMC compliance subject matter experts without first fundamentally understanding their governing resources.

Reading and interpreting old and new requirements, comparing them to existing documentation, and understanding how each change affected a client's security posture helped solidify my growth and proficiency concerning written regulations. My exposure to policies and security frameworks at ODU made that process more approachable, even though the scale and detail were much greater in a professional setting. The internship forced me to grow quickly in this area, and by the end, I felt much more comfortable navigating compliance frameworks and understanding how they dance around business operations.

My digital forensics coursework didn't directly relate to the specific work I did at Valor, but some of the attention to detail requirements carried over. In digital forensics, you learn how to examine evidence without overlooking small details. I was able to practice this during guided labs that often required a keen sense of attention to detail. The same approach was applied to compliance documentation to ensure accuracy and professionalism. A misplaced sentence, an unneeded security recommendation, or an outdated control reference can spark confusion or misalignment in a client's paperwork. The discipline I applied in my forensics labs helped me slow down and treat documentation with the same precision.

One of the biggest connections I noticed was between my networking courses and the work I did exploring cloud computing services and Microsoft Azure. At ODU, I learned about networking fundamentals through the lens of local hosts; wired and wireless connections, hardware, data centers, and so on. Unknowingly, my exposure to the concept of cloud computing was borderline. Once I learned that cloud computing was not rocket science, but simply a model of computing that provides on-demand resources, I realized I may not have been exposed to it explicitly at ODU, but I've tiptoed near the concept unknowingly.

The ValorVictor project required me to work through how Azure services would support authentication, storage, access control, and compliance requirements. This experience brought the networking fundamentals I learned in class into focus. First, I was focused on the concept of cloud computing and how it worked. Shortly after, my focus shifted to how I could design a secure, client-facing portal while aligning with CMMC controls. That connection to the foundational knowledge of networking that Jackson continuously emphasized helped me gradually build my familiarity with cloud computing and helped me understand it at a deeper level.

Another gap I noticed during my internship concerned business integration. ODU's undergraduate program heavily focused on technical skills, respectively, but failed to explore much on how cybersecurity interacts with real organizational constraints. I was not exposed to balancing technical best practices with business budgets, personnel limitations, or operational workflows; however, working at Valor demonstrated that these restrictions and realities shape cybersecurity decisions just as much as technical knowledge does. Through Jackson, communication skills and the ability to explain technical concepts to non-technical clients were highlighted as being just as important as understanding the concepts themselves through several conversations we shared.

Overall, the internship allowed me to connect my education through ODU with real-world practice in a smooth and natural way. Some parts of my academic experience prepared me directly, while other areas required more training on the job, however the combination of both helped me grow as a confident cybersecurity professional. The internship filled gaps in my knowledge, reinforced and built upon the foundation I built at ODU, and helped me apply my academic knowledge in a practical work environment.

Learning Objectives

At the start of my internship, I set four learning objectives that I anticipated growth with through my internship at Valor. These goals focused on developing technical depth, gaining compliance exposure, strengthening my understanding of risk, and learning how cybersecurity fits into business operations. Reflecting on my time with Valor Cybersecurity, it's clear to me how each objective was strengthened through my work and exposure.

Objective 1: Developing Scalable Security Solutions

For this objective, I wanted the opportunity to work with modern cloud environments and understand how scalable security solutions are designed. During the early weeks of the internship, I spent a lot of time researching Azure services, cloud architecture models, and best practices for building secure, flexible systems. Despite not having enough time to carefully orchestrate and carry out the building process, I still consider this objective a success. It was also meaningful, as I wasn't working on this project in isolation. Jackson provided advice, guidance, and a point of contact to bounce ideas around with. Everything I researched had to tie back to Valor's business needs and compliance expectations, and with Jackson's support, this project became a fully immersive, team-building exercise that conditioned my cloud knowledge, planning skills, and introduction to Valor's operations.

Planning the ValorVictor project encouraged me to think about scalability from both a technical and organizational perspective. It wasn't simply about "using Azure" but about ensuring the platform design supported secure workflows, client accessibility, and long-term growth. Mapping out how authentication, storage, and access control would work in an Azure cloud

environment helped me build a practical understanding of scalable solutions and shifted my perspective to consider things like data flow, various user roles, and audit requirements. This significantly strengthened my ability to think in terms of both technology and business needs.

Objective 2: Threat Analysis, Compliance, & Risk Management

This objective was fulfilled through almost every task concerning documentation, gap assessments, and CMMC revisions. Instead of studying threats and controls in a classroom environment, I had to analyze client documentation, identify gaps, determine whether clients were meeting security requirements, and recommend resources and changes to their posture to ensure they remained secure and within compliance.

The transition from Rev. 2 to Rev. 3 was a huge opportunity to build this skill. Revision 3 introduced new requirements and shifted how certain controls were interpreted, which led me to consider potential risks clients might face with outdated policies. Each outdated policy, missing control, or incomplete explanation in their paperwork represented a potential weak spot.

Objective 3: CMMC Framework Familiarization

Objective 3 was fulfilled more than any other. Before the internship, my knowledge of CMMC was limited to a general awareness that it existed. I had never worked with the framework directly, but over the course of the internship, CMMC became the center of almost everything I did. I reviewed dozens of controls, updated documents to reflect Revision 3 updates, interpreted client cyber environments through the lens of CMMC's framework, and helped build materials that ensured compliance readiness.

I also gained a deeper understanding of some challenges that small businesses face when attempting to comply with a mandated framework. Clients would often have limited staff, other priorities, and varying levels of technical competence. My experience at Valor taught me how to balance completeness with practicality.

Upon reflection, I believe each objective I set at the beginning of the internship was fulfilled to some degree. I gained technical exposure, compliance expertise, risk awareness, and a strong understanding of how business and cybersecurity decisions affect one another.

Aspects of Interning at Valor

Most Motivating

There were various moments at Valor where I could feel myself growing the most, where I could see the impact of my work, or where I realized that I was exactly where I wanted to be, with a team I wanted alongside myself. The immersive and collaborative responsibilities, along with the mentorship I received from Greg and Jackson, both played a role in shaping those moments.

One of the most exciting aspects of the internship was seeing the work I did directly supported the team and our clients. Everything I worked on had an immediate purpose: updating a security plan, reorganizing documentation, or seeing newly updated documentation fill up a folder. Seeing my contributions and knowing that I'm directly helping fulfill my team's list of to-do's while getting our clients one step closer to compliance gave the work purpose and made it feel meaningful. That sense of purpose motivated me every day and allowed me to deeply appreciate the type of work I was doing.

Another motivating part of the internship was the collaboration and mentorship I experienced with Jackson and Greg. Being able to converse with individuals that I admire, with deep technical knowledge, boasting impressive resumes of experience, gave me motivating and valuable insights. Jackson's approach to time management and his work philosophies directly influenced how I approached my own work and how I view my career. Jackson was transparent about the challenges he experienced, and Greg was continuously transparent about what the job required and what he expected from me, helping me set realistic expectations and goals for myself. Conversations with them always left me feeling proud, energized, and inspired to continue improving.

Most Discouraging

Despite my internship at Valor being incredibly valuable, there were a few moments that felt discouraging or difficult from my perspective. These moments did not take away from my experience but instead challenged me in ways I didn't anticipate and forced me to adapt and grow.

To my surprise, the most discouraging aspects stemmed from the remote nature of the internship. My initial reaction after discovering my internship was remote was optimistic and excited. My prior position was mostly in-person, but I cherished the few moments we were afforded to work remotely. I quickly realized that the completely remote environment sometimes felt more isolating than a hybrid internship might have felt. It was impractical to work anywhere without multiple monitors, so I was left with no choice but to sit in my home office, working, studying, and watching the day pass by. Sometimes I reminisced about my old commute, watching the sky glow slowly as the sun rose or seeing the trees change along with the seasons.

While modern software, such as Teams, along with Valor's culture, made it easy to stay connected virtually, there were moments I wished I could be in the same room as the team, ask questions face-to-face, or even observe conversations in person, especially at the beginning of the internship while I was freshly navigating everything. Eventually, after supplemental meetings and calls, I felt independent and knowledgeable enough to carry out my duties without feeling lost or confused; though, I still had my moments.

These moments were by far the most discouraging; however, they demanded reflection and contributed to the lessons I carried away. The privilege of being able to work remotely and the opportunities that stemmed from it are far too great to ignore, and while there were moments during the internship that felt lonely and discouraging, it was an opportunity to adapt by sharpening my discipline and strengthening my independence. Growth rarely happens without difficulty, and I eventually grew to appreciate the remote nature of my work in ways I hadn't prior.

Recommendations for Future Interns

Cybersecurity internships can vary widely depending on the organization, but for a small business like Valor, preparation and mindset could make all the difference between success and failure.

The first recommendation echoes from Jackson's advice: build a strong foundation in the basics. No matter what area of cybersecurity you plan to go into, understanding core concepts like networking, authentication, access control, encryption, and operating systems is essential. These fundamentals come up every day in client documentation, policy reviews, and compliance work, so anything more technical than policy will more likely lean heavily on your understanding of

those foundational concepts. Understanding how systems communicate, how accounts are secured, and how data moves within an organization before starting the internship will help everything else make sense and fall into place.

My second recommendation for interning at Valor is to have at the very least a dual monitor setup. Working with documentation, research notes, CMMC controls, emails, and reference materials all at once is extremely difficult on a single screen. A second monitor makes it easier to compare documents, view multiple tabs, follow along during meetings, and keep your workspace organized. The difference in productivity and comfort is huge for any intern working in cybersecurity or policy.

Lastly, I'd recommend developing a strong sense of independence. In a small business, there isn't always time for someone to walk and talk you through each detail. You will need to research things on your own, navigate problems, and make educated decisions. It's also important to be proactive about asking questions, but it's just as important to try to figure things out on your own. Many of the skills I learned came from taking the initiative: thoroughly reading documentation, reviewing CMMC materials, or researching Azure tools before asking for help. Having a good combination of independence and curiosity will make you a valuable team member.

Conclusion

My internship at Valor Cybersecurity ended up being one of the most meaningful experiences of my undergraduate experience, especially considering how unexpectedly it came into my life. I've learned how policy formation, cloud architecture, compliance requirements, and business operations all connect to form the foundation of an organization's security posture. All

of the work I collaborated on and completed provided me with technical exposure that I would have never been able to earn through just coursework.

My experience reshaped my perspective about my time at Old Dominion University. I see how the subjects I was introduced to connect to the responsibilities I was given during the internship. The mentorship I received throughout my time has helped me understand not only the technical side of the field but also the habits and mindset needed to be valuable and effective in cybersecurity. The internship strengthened my confidence and even helped clarify the areas of cybersecurity I want to continue learning in: cloud security, compliance, and architecture.

Looking ahead, I have a clear vision of the type of roles I want to pursue and the skills I need to build to get there. Valor taught me how dynamic cybersecurity is and how important it is to remain adaptable, curious, and willing to keep learning. Even though the internship wasn't the one I originally planned for, it unexpectedly ended up preparing me for the next chapter of my career.