Michael Opoku-Arthur
August 2, 2025
Leidos- Cybersecurity and Information Assurance Intern
CYSE 368/Internship
Summer 2025

Table of Contents

Introduction

As someone who has had the opportunity to obtain an internship every year since entering college, I have gained the foundational knowledge of my ideal working environment and have learned to differentiate between a company that can help me achieve my goals and one that cannot. Accepting an internship at Leidos was a decision influenced by my career aspirations and the potential for growth within the company. Although I had an offer to return to a previous internship, I opted for Leidos because I believed the ceiling for advancement was higher, and I had the opportunity to explore my minor in cyber risk management.

After being assigned to my team, my primary learning objectives for this internship were as follows: First, I aimed to gain a comprehensive understanding of the Department of Defense's Risk Management Framework (RMF) and how it aligns cybersecurity policies and practices, this was an area aligned closely with my minor in Risk Management and represented a pivot from purely technical cybersecurity work to a more compliance-focused approach.

Second, I hoped to obtain practical experience performing cybersecurity control audits and assessments.

Third, I wanted to experience firsthand the full lifecycle of obtaining and maintaining an Authorization to Operate (ATO) for Department of Defense information systems.

In this final paper, I plan to reflect on my experiences, challenges, and growth throughout my internship with Leidos on the Air Force National Capitol Region (AFNCR) contract. This paper will explore the contract environment, my daily responsibilities, the application of academic knowledge, and how this experience informs my future professional and educational journey.

Leidos is a global company specializing in technology and engineering services, significantly emphasizing defense, intelligence, and civil government sectors. The company is divided into five sectors, each focusing on a different mission within the workspace. I found myself in the Digital Modernization sector, one of the largest sectors, with a mission to bring together digital transformation and information technology. Leidos is a Fortune 500 company and has grown to be one of, if not the biggest, government contractors nationwide.

The Air Force Network Communications Region (AFNCR) contract maintains the security and reliability of the United States Air Force's communications and IT systems. This includes ensuring secure networks, protecting sensitive data, and maintaining compliance with federal cybersecurity mandates.

This contract involved working with government agencies demanding security requirements, meaning employees operate in highly regulated environments. My workspace was within a Sensitive Compartmented Information Facility (SCIF), a secured room to prevent data leakage. Within this environment, strict rules apply, such as prohibitions on personal electronics and rigorous identity verification. The SCIF embodies the company's commitment to national security and reflects the serious nature of the work. In short, no outside technologies were allowed, such as cell phones, personal computers, smart watches, Bluetooth-enabled devices, and anything that can record audio and/or video. For once, I had found myself in unfamiliar territory. I had to navigate a work style that required being away from outside technologies and communications for eight hours daily.

My internship began with a prolonged orientation and onboarding phase typical of government contractors handling sensitive information. Due to being on a contract, I had to orient twice; once for Leidos corporate and again for AFNCR operations. For the corporate side, things were streamlined; it involved the standard onboarding orientation, compliance training, resources, etc. However, for the contract, onboarding is when things began to get frustrating. I'm unsure if this applies to all contracts, but there is no pre-onboarding for my contract. This means that everything starts on your first day on-site. Typically, your laptop and account may be ready for you on the first day, but this wasn't the case. My laptop request and account creation process did not begin until my first day. Due to these delays, my first several weeks were extremely challenging, which limited my ability to engage fully with the work. This situation tested my patience and professionalism early on, as I had to remain motivated without access to necessary tools. The pace of things often left me irritated, especially when the response to my frustration was "that's just how government goes". However, I persevered and kept my composure while playing the waiting game.

Despite these initial obstacles, the orientation was thorough and informative. I completed multiple computer-based trainings (CBTs) focused on security policies, compliance frameworks, and specific government standards. These trainings provided a solid foundation for understanding the Risk Management Framework (RMF) that governs cybersecurity within the Department of Defense.

I shadowed team members during this phase and absorbed company culture and expectations. The slow start allowed me to focus on absorbing policy materials and understanding the regulatory environment that shapes the company's operations.

When I finally received access and was assigned to the Authorization & Assessment (A&A) team, the internship experience accelerated. My team lead, Meredith, was supportive and eager to involve me in meaningful work, helping me understand how my role fit into the larger risk management lifecycle.

Management Environment

Due to being on a contract and dealing with a customer (Air Force), I did not deal with any corporate management after my orientation. I joined this contract during a weird phase for my department; my manager, who hired me, James, was leaving the contract for another. James was only temporary, as he was sitting in place for Lauren, the manager, on an extended emergency leave. My first day was also Lauren's first day. To this date, I haven't had much interaction with Lauren; it was almost as if I were invisible to her. This was quite unfortunate for me, as the other interns in other departments had hands-on managers who were eager to see them excel during their time on the contract. The office environment in my department seemed divided to me; teams only spoke and met with each other. Although we were all under the Cybersecurity Department, it was unfortunate to see how this was. Compared to my previous internship, although we were in the IT department and everyone had a different function, our manager still ensured that we had department meetings and were a family because his motto was that we had to stick together. So I blamed the divided office environment on the manager.

After being assigned to my team, Meredith, my team leader, played an essential role in my professional development. She balanced close supervision with autonomy, allowing me to grow while providing guidance when needed. Regular check-ins ensured alignment on tasks and progress, and she fostered an environment where questions and learning were encouraged. In my head, Meredith was my real manager.

The team utilized communication platforms like Microsoft Teams and ShareFile to manage projects and share documentation securely. Although the overarching managing environment did not support my growth, working closely with Meredith allowed me to excel as she provided structure, resources, and mentorship critical for navigating the complex cybersecurity risk management regulatory framework.

Major Work Duties and Projects

A core component of my internship involved understanding and applying the Risk Management Framework (RMF), a six-step process developed by the National Institute of Standards and Technology (NIST). Their frameworks are widely accepted as the standard, and the RMF Lifecycle Process was adopted and used by the Department of Defense to manage cybersecurity risk.

I began by studying NIST Special Publications 800-37 and 800-53, along with Department of Defense Instruction (DODI) 8510.01. DODI 8510.01 was the DoD adopted framework of NIST RMF. These documents provided the foundation and listed the steps for managing risk in DOD information systems, detailing the security controls necessary for compliance. Although I would only be working with the Assess and Authorization steps, Meredith wanted to understand the whole approach, which I am grateful for, as I could understand the entire process holistically.

Once familiar with these frameworks, I audited cybersecurity controls categorized into control families. There are eighteen control families in which 256 security and privacy controls are dispersed. We must have a security plan for each control family; each plan must address the guidelines listed in the DODI 8510.01 and the other NIST frameworks. Using these plans, I would begin my auditing process. These were practice audits, as the real audits only happen when we actively try to renew or achieve an ATO (Authorization to Operate). We had an ATO renewal approaching in December. Early in the internship, I worked with less complex families such as Physical and Environmental Protection (PE) and Awareness and Training (AT), which involve controls over physical access and security awareness programs.

As my proficiency increased, I was assigned to more technical families, including Configuration Management (CM) and System and Information Integrity (SI). These required detailed assessments of system settings, integrity protections, and monitoring mechanisms.

Auditing involved cross-referencing control requirements with organizational plans and evidence, often housed in eMASS or ShareFile repositories. Each control required validation to determine whether it was fully implemented, partially compliant, or not met. I used color-coded spreadsheets to track compliance status. The color coding was to tell myself whether I was doing it correctly, incorrectly, or confused. The colors were green, red, and orange.

One of the most challenging projects was auditing the SI control family, which required many artifacts as supplemental guidance beyond control plans. Although I initially struggled due to incomplete eMASS access, I worked closely with my team lead to obtain the necessary artifacts and complete my assessments.

These tasks sharpened my analytical skills, attention to detail, and understanding of cybersecurity policies operationalized in a real-world government setting.

Use of Cybersecurity Skills and Knowledge

Before starting this internship, my cybersecurity knowledge was primarily technical, focused on network security, threat detection, and incident response from prior internships and coursework. However, Leidos expanded my perspective by emphasizing compliance, policy, and risk management. As mentioned in the introduction, one of the primary reasons for accepting this internship was that it would allow me to explore my minor in risk management. I was interested in eventually becoming a cyber risk manager later in my career, but although there was interest, I had never received any exposure outside of the classroom. Through this internship with Leidos, I confirmed internally that I wouldn’t mind venturing into this line of work.

The RMF framework introduced me to a structured methodology for evaluating and managing cybersecurity risk. Learning about the specific security controls and their categorization helped me understand the layers of defense required in government systems.

My auditing work required familiarity with documentation, standards, and governance frameworks. Technical skills weren’t needed, but they often let you understand what happens whenever complications arise. For example, say you’ve reached out to a team to let them know that their firewall is non-compliant due to an open port, the team may reach back out and let you know that if they use what is required to ensure compliance, then the firewall may not work correctly if that port is closed. As a security auditor with technical expertise, you can better understand the issue rather than just telling the team to “figure it out”. This is why I want to gain as many technical skills as possible before managing risk. I often hear the saying, “How can you manage a team if you’ve never been in the fields before?”.

Additionally, I improved my skills in using specialized compliance tools such as eMASS, navigating control libraries, audit templates, and evidence repositories. This hands-on experience was invaluable, as such tools are industry standards for government contractors.

Throughout the internship, I enhanced my communication skills by regularly discussing findings with supervisors, asking clarifying questions, and documenting detailed reports—this combination of technical, analytical, and interpersonal skills enriched my professional toolkit.

Connection to ODU Curriculum

My academic background at Old Dominion University prepared me well for many aspects of this internship. Coursework in cybersecurity fundamentals, network security, and risk management laid a foundation for understanding core concepts applied at Leidos. I always say that it is one thing to learn in the classroom, but to use what you’re learning in the real world is the real eye-opener. I’m incredibly grateful for internships, as I can apply what I know in the classroom to real life. The best part about this is that I can pivot into something else the following year if I didn't enjoy it. This is an opportunity you must take advantage of as an undergrad because once you enter the real world, you may find it more difficult to navigate using this method.

Back to the topic of the connection of the ODU curriculum, the classes under my minor allowed me to understand risk management. The cyber risk management elective course also mentioned the various frameworks I would work with and risk governance in a cybersecurity setting. These classes correlated strongly with the RMF frameworks and compliance assessments I conducted.

However, the internship also revealed new concepts and real-world complexities beyond classroom theory. The intricate process of Authorization to Operate (ATO) and the detailed audit procedures required a deeper appreciation of government regulations and bureaucratic workflows.

Furthermore, my curriculum did not cover the use of specialized software like eMASS, underscoring the value of on-the-job learning.

Overall, the internship complemented my education by reinforcing theoretical knowledge, introducing new practical skills, and highlighting the importance of adaptability in a professional environment.

Internship Outcome Fulfillment

Reflecting on my initial objectives, I see that my goals were fulfilled to a certain extent. My objectives were as follows:

- Gain a thorough understanding of the RMF and how it structures cybersecurity risk management within the Department of Defense.
- Obtained hands-on experience auditing security controls and managing compliance documentation, building skills essential for a cyber risk management career.
- Participate in an Authorization to Operate (ATO) renewal process.

My first objective was fulfilled to its entirety. Through completing the CBTs (Computer-Based Trainings) and thoroughly reading through the different frameworks provided, I was able to gain a strong foundational understanding of the Risk Management Framework (RMF) and how it applies specifically to Department of Defense (DoD) information systems. Before this internship, my knowledge of RMF was limited to surface-level definitions and theory. Still, now I can confidently discuss its components, steps, and significance in maintaining the cybersecurity posture of federal systems. Each training module not only introduced me to new terms and processes, but also helped me see how the RMF guides every aspect of security, from categorizing systems to selecting and implementing the proper controls, all the way to continuous monitoring. I am an individual who asks a lot of questions, as curiosity and clarity are essential to truly mastering a subject. In this regard, having a team lead like Meredith significantly impacted my learning experience. She consistently demonstrated patience, support, and encouragement, regardless of how often I sought clarification or further explanation. Her willingness to walk me through different scenarios, offer context, and point me toward additional resources made learning RMF less daunting and more engaging. It was truly amazing to have someone who understood the material and cared about ensuring that I understood it. That kind of mentorship elevated my experience and gave me confidence in navigating complex frameworks like RMF in a real-world setting.
Additionally, the internship offered exposure to a government contractor’s operations, enhancing my knowledge of working in a highly regulated, security-conscious environment.

My second objective was only halfway fulfilled. While I did have the opportunity to gain practical experience with control audit assessments, the nature of the work I was assigned made it more of a simulated or practice-based expertise rather than a fully hands-on, real-time evaluation. Essentially, I was reviewing and assessing control implementations that had already been audited by someone else, which meant my work functioned more as a learning tool than a genuine contribution to a live project. This setup was still valuable, as it allowed me to apply the knowledge I had gained from the CBTs and RMF readings to actual scenarios. It helped me understand how to examine evidence, interpret control requirements, and document findings in a format aligned with federal and DoD standards. However, this approach also came with limitations. Since the assessments were hypothetical, I wasn't exposed to the whole decision-making process or the real-time collaboration that often happens during a live evaluation. At times, I felt restricted in what I could access due to the sensitive nature of the environment. Not having full access to all artifacts sometimes made it difficult to understand the full context behind certain control implementations or how specific security objectives were being met. While I developed a firmer grasp of the audit process and learned how to approach control reviews methodically, I recognize that the learning would have been more complete if I had engaged with ongoing, in-progress assessments with unrestricted artifact visibility. Overall, the experience laid a solid foundation and prepared me for future roles where I may be given more access and responsibility.

My final objective of working on a live ATO renewal was not fully realized within the internship timeframe. This was mainly due to the timing and nature of the projects my team members had to tend to. Despite this, I don't view this as a loss. The foundational skills I acquired, from understanding the Risk Management Framework (RMF) and learning the purpose and structure of ATO packages, to reviewing example assessments and practicing control evaluations, have given me a strong starting point. I now have the vocabulary, context, and technical understanding to step into future roles and quickly adapt to working on live ATO efforts. This internship has laid the groundwork, and I am confident that with more time and continued exposure, I will be fully prepared to contribute to these processes in a meaningful way.

Motivating Aspects

The most motivating aspect of this internship was the trust that was placed in me to handle complex compliance-related tasks. Early on, I expected to be limited to observational duties or more administrative support, but I was surprised when I was gradually entrusted with increasingly technical responsibilities. One of the most affirming moments came when I was promoted to audit more advanced and technical control families. Along with this responsibility came access to sensitive documentation and systems, which reflected to me the confidence that Meredith had in my abilities. That trust validated my skills and pushed me to take my learning more seriously and dig deeper into the material. It motivated me to enhance my understanding of cybersecurity controls, documentation standards, and how each element fits into broader compliance efforts under RMF.

Another significant highlight of my internship experience was attending intern-focused events at the Leidos headquarters. These events gave me a broader view of the company's culture and mission beyond my day-to-day responsibilities. One of the most memorable moments was getting the chance to meet the CEO and several senior leaders.

Hearing from them about the company’s strategic direction, values, and commitment to innovation helped me see how my work contributes to a larger picture. It fostered a genuine sense of belonging and purpose, making me feel like more than just an intern. These interactions made it clear that Leidos is not just a place that values technical competence, but also personal development, vision alignment, and team collaboration. The trust in my work and the broader exposure to leadership helped make this internship an incredibly motivating and enriching experience. Although I wasn’t pleased with the workplace culture on my specific contract, I could tell that it did not truly reflect the overall mission and culture that the company had to bring. Attending these corporate events reinforced the type of workplace environment I would like to work in following graduation. Following these events, I began to take advantage and start networking with employees on the corporate side, primarily trying to understand corporate operations and what positions to seek. One thing I found out is that corporate IT is called CIS, or corporate information security. This was a significant achievement as I searched in and out to figure out the internal IT operations.

Challenging Aspects

Although there were many positives, the internship was not without its challenges, which mainly stemmed initially. One of the most frustrating aspects was the slow start due to access delays. I spent several weeks waiting for system accounts to be provisioned and for my equipment to arrive. I was eager to contribute and dive into the work during that time, but the lack of access significantly limited what I could do. This tested my patience and created an initial sense of disconnect from the team and the overall mission of the internship. It was challenging to feel like I was falling behind or waiting on the sidelines during such a short and critical professional development period.

Beyond access issues, compliance audits’ complexity and detail-oriented nature also posed a steep learning curve. Regulatory frameworks, particularly those aligned with the Department of Defense, are filled with dense and particular language that can be difficult to interpret without experience. Auditing and evaluating hundreds of controls across various families required sustained mental focus, attention to detail, and the ability to navigate. There were times when I had to read through documentation multiple times to understand the requirements being addressed, let alone assess them. Additionally, technical limitations in some of the tools we used and restricted access to certain artifacts slowed my ability to engage with audit tasks fully. These hurdles required creative problem-solving, persistence, and constant communication with Meredith to fill the gaps.

These are all challenges I would have hoped not to face, especially considering this was my final internship before entering the workforce. I had envisioned a smoother, more immersive experience where I could hit the ground running. However, in hindsight, I recognize that these obstacles taught me essential lessons in resilience and adaptability. I learned how to remain focused and committed even when progress was slow and to keep a positive mindset in the face of unexpected setbacks. These experiences will serve me well in future roles, where things will not always go according to plan. They reminded me that professional growth often comes from navigating discomfort and uncertainty.

Recommendations for Future Interns

For future interns entering the cybersecurity and compliance field, especially within a government contracting environment, I would offer several key takeaways to help them make the most of their experience.

First, come in with patience and a flexible mindset. From what I've experienced, government contracting environments, particularly those involving the Department of Defense, have strict onboarding procedures and security protocols that can delay your access to systems and equipment. This can be discouraging initially, especially when you're eager to contribute. However, developing patience and adaptability during this period is essential. Instead of moping around, wondering when your time will come, use that downtime productively by engaging in foundational trainings, reading internal documentation, and familiarizing yourself with the broader context of your role.

It's also essential to develop a solid understanding of key cybersecurity frameworks and policies early on. Interns should aim to grasp the fundamentals of NIST 800-37 and NIST 800-53, along with DoD-specific guidance such as DODI 8510.01. These documents are cornerstones in federal cybersecurity compliance and risk management, and having a working knowledge of them will make your tasks more meaningful and manageable. You should also invest time in understanding risk management concepts and core auditing principles, as much of your work will involve interpreting complex compliance language, assessing implementation of controls, and reviewing documentation for accuracy and completeness.

Organizational and documentation skills are also critical. Auditing and compliance work often involves managing large amounts of information across many control families. Keeping your work structured, clearly documented, and easy to follow helps your team and strengthens your professional discipline. Equally important is the ability to proactively communicate with your supervisors and team members. Don't hesitate to ask questions or request guidance if something is unclear, whether it's a technical concept, task expectation, or access issue. Open communication can prevent unnecessary delays and show your team you're invested in correctly doing the work.

As your responsibilities grow, you may be trusted with more technical tasks or access to sensitive documentation, just as I was. These opportunities enrich and can build your confidence, so always be ready to step up. To that end, I recommend taking full advantage of training resources early and approaching every assignment with a growth mindset. The most progress comes when you're willing to stretch beyond your comfort zone, seek feedback, and apply lessons learned.

In short, preparation in these areas will position you to hit the ground running and make meaningful contributions. While challenges may arise, embrace them. They are also valuable learning experiences. If you're in a position like mine, where this may be one of your final internships before transitioning into the workforce, how you respond to these situations will shape not only your experience but your long-term professional development.

Conclusion

To conclude, my internship experience at Leidos has been both transformative and enlightening, marking a significant milestone in my professional development and academic journey. Coming into this internship, I had foundational knowledge in cybersecurity, primarily technical skills gained through coursework and previous internships. However, this opportunity broadened my understanding by immersing myself in the Department of Defense's Risk Management Framework (RMF) and exploring cybersecurity from a compliance and risk management perspective. This pivot aligned closely with my minor in Cyber Risk Management and gave me a clearer vision of my future career path.

Although the internship began with considerable challenges, including delayed system access and equipment provisioning, these initial setbacks taught me invaluable lessons in patience, resilience, and professionalism. Navigating the highly regulated, security-conscious environment of the Air Force Network Communications Region (AFNCR) contract required adaptability and a strong commitment to maintaining focus despite obstacles. The unique constraints of working within a Sensitive Compartmented Information Facility (SCIF) and adhering to strict protocols reflected the seriousness and importance of the work being done to protect national security.

A critical highlight of the internship was the mentorship and guidance I received from my team lead, Meredith. Her support helped me develop confidence in a complex and demanding work environment. Through her, I gained hands-on experience auditing security controls, understanding the intricacies of federal cybersecurity policies, and using industry-standard tools like eMASS. The practical application of frameworks such as NIST SP 800-37 and 800-53, alongside Department of Defense Instruction 8510.01, provided a comprehensive view of cybersecurity risk management processes that go well beyond textbook theory.

One of the most rewarding aspects was the gradual increase in responsibility, which motivated me to deepen my technical knowledge and hone my analytical skills. This experience reaffirmed my interest in pursuing cyber risk management as a career, highlighting how essential it is to pair technical expertise with an understanding of governance, compliance, and policy. The internship also reinforced the critical role of effective communication in cybersecurity roles.

Despite not fully participating in a live Authorization to Operate (ATO) renewal during the internship, my exposure to the ATO lifecycle and compliance documentation provided a strong foundation for future professional endeavors. I now possess the vocabulary, contextual understanding, and procedural insight to approach such projects confidently. This internship has equipped me with practical skills and instilled an appreciation for the complexities of cybersecurity governance in government contracting.

In addition, my experience illuminated the realities of workplace culture and management dynamics. While I encountered some challenges related to team cohesion and managerial support, these situations fostered my ability to work independently and proactively seek out mentorship. I learned that professional growth is often driven by one's initiative to overcome environmental limitations and find allies who support development.

Reflecting on the connection between this internship and my academic preparation at Old Dominion University, I appreciate how coursework laid the groundwork while real-world experience filled in gaps that only hands-on practice can address. This internship demonstrated the value of integrating classroom learning with professional exposure, encouraging me to continue leveraging both as I advance in my career.

Overall, my time at Leidos has been an enriching, challenging, and motivating experience. It tested my patience, sharpened my skills, and expanded my professional outlook. I am grateful for the trust placed in me, the mentorship I received, and the opportunity to contribute meaningfully to a critical mission. This experience has strengthened my commitment to becoming a cyber risk manager and prepared me to navigate future challenges in the cybersecurity field confidently. I am excited to build upon this foundation, continue learning, and take on greater responsibilities. The lessons learned throughout this internship will be a valuable compass as I transition from student to cybersecurity professional dedicated to safeguarding information systems in increasingly complex environments.