

Telos Internship

Employer: Olive

By: WAWERU, IAN

12,1,2023

CYSE 368 Fall 2023

**Table of contents**

1. Page 3: is the Introduction
2. Page 3: Why did I decide to do an internship in this business or organization?
3. Page 3& 4: “Explain at least 3 specific learning outcomes or objectives you hope to achieve in your internship.
4. Pages 4 -6: “Describe the beginning of your internship.”
5. Page 6: “Describe the management environment at the internship.”
6. Pages 6-7: “Describe in detail your major work duties, assignments, and projects.”
7. Page 6-7: “Discuss your specific use of skills or knowledge of cybersecurity in the internship.”
8. Page 7: ODU curriculum preparation
9. Pages 8: Motivating, Discouraging, and challenging aspects of the internship.
10. Page 8: Conclusion

**Internship final**

College has shown me many things and has helped me grow as an individual. I’ve been going to Old Dominion University for five years now and I hope this year is my last. Coming into college, I had no idea what I was getting myself into. I wanted to try a multitude of different studies, but I wasn’t sure which one fit me the best. For instance, I wanted to learn more about marine biology because I like the ocean, and I found it interesting how we haven’t explored everything yet. I lost passion in trying to learn this study and It’s not easy to find a job for that subject. After thinking about what I wanted to do for a while, I eventually decided I wanted to learn more about cybersecurity. There are a multitude of reasons as to why I chose this field. One reason I wanted to learn more about cybersecurity is because of my mother and her current husband. My stepfather works for a company that prioritizes cybersecurity, he told me about it and he is one of the main authorities in this company. Another reason I chose cyber security was because of where I live. I’m from Northern Virginia and there are plenty of jobs that require my profession. Washington DC is also nearby, and this city has a bunch of different cybersecurity jobs available. It was starting to make sense to me, and I committed to it going into my freshman year. I started working as an intern during the summer after my sophomore year. The organization I started interning for is called Telos. This place is the same company that my stepfather told me about. I was introduced to Telos by my stepfather, at the time I was looking for a summer job so I could save up before I headed back to school. When I started, I was not working on anything about cybersecurity. I was working in the facility department; I helped the building manager maintain the entire building. I liked working in this department, I got to learn a lot of different things when it comes to maintaining a building. It was a lot of work and required a lot of heavy lifting. However, after learning more about cybersecurity, I noticed what I did was technically teaching me a little bit about cybersecurity. For example, we have doors that require an ID badge to get into certain places in the building. It was our job to fix issues such as that one that can occur. Another example of what I did in facilities was empty out a multitude of shelves that had cybersecurity data from a long time ago. It’s important to shred paperwork because we don’t want any information to leak, even if they aren’t useful anymore it’s still a risk factor. Telos was built in 1968, and some documents came from as long as that. I’ve been an intern for a couple of years now and I started working at facilities in my sophomore year and that year was also 2020. It was difficult at the time to do anything, especially for facilities. In the summer of 2021, I came back, and I became an intern again for Telos. I was still working with the facilities department, but I got a better experience since it was the back end of the pandemic. It was short but I felt like I learned a lot in the time I had with facilities. The next summer arrives, and it is 2022. I am again interning for Telos, however, this time around my stepfather pulled me out of facilities and added me to a group that disciplines in cybersecurity. You can only intern at Telos twice; however, this is technically my first time working on cybersecurity and I had a COVID year that pretty much didn’t count. It was like a fresh start, and I was nervous before starting because this would be my first time handling government work. I set a couple of specific learning objectives to guide my experience and ensure that I could maximize the opportunities presented. I wanted to develop practical cybersecurity skills, enhance communication and collaboration skills, and gain insight into compliance and regulations. Learning practical cybersecurity skills includes understanding and implementing security measures, identifying vulnerabilities, and participating in risk assessment and mitigation. Communication and collaboration skills is an essential aspect of working in any organization. I aim to improve my ability to collaborate with colleagues and communicate whenever I get stuck or need help understanding something. I know Telos excels in providing solutions for regulatory compliance, and I aim to gain an understanding of that and many more. Two weeks later I was added to the content development team. My stepfather, one of my many bosses, introduced me to one of the main authorities working in this department. Her name is Olive, and she is my new boss for the rest of the summer. We held a meeting, and she gave me a rundown about the company and what content management does for Telos. When we held this meeting, I got to learn a lot about the history of telos, major products, major customers, etc.

**History**



This organization is a prominent cybersecurity and information technology solutions company. The one I reside at was founded in 1969 and it has a long-standing history of providing innovative solutions for securing and protecting critical infrastructure, information, and assets. I find that interesting because I wouldn’t have thought much about cybersecurity in the 70’s. Telos has grown to become a trusted partner for government and commercial clients seeking cutting-edge technology solutions. Telos is an organization that offers a wide range of products and services in the fields of cybersecurity, risk management, compliance, and identity management. These solutions are designed to help organizations protect their critical assets, secure their information, and meet regulatory requirements.

**Telos Product/Services**



One of Telos' key products is the XACTA suite. The Xacta suite is comprised of X360 and Xacta.io. X360 is the flagship product, a risk management tool that automates and facilitates assessment and authorization processes. The tool also automates processes around remediation and ongoing compliance. Xacta.io, on the other hand, consolidates scan results from multiple sources and correlates these to controls and requirements under a regulation or across multiple regulations that are relevant to an organization. The correlated and consolidated data can be sent to X360 to depict the organization's compliance posture, and from there derive data to understand its vulnerabilities, risks, and the necessary remediation needed to build a better security posture. My stepfather helped create this website, it is a cloud-based security and compliance solution that offers a unified view of an organization’s risk and compliance landscape. It streamlines security operations, risk management, and compliance efforts across the enterprise.

**Major Customers**

Telos serves a diverse client base, including government agencies, defense organizations, critical infrastructure providers, and commercial enterprises. Their expertise in regulatory compliance, secure communications, and identity verification makes them an essential partner for clients with stringent security and compliance requirements. Telos has a strong presence in a couple of sectors: Government agencies, Critical infrastructure providers, Commercial enterprises, and defense/military organizations.

**Government agencies**

Telos works closely with various U.S. governments, including those within the Department of Defense (DoD), the intelligence community, civilian agencies, and law enforcement organizations. They provide cybersecurity compliance, and risk management solutions to help government agencies protect critical infrastructure and sensitive information.

**Critical Infrastructure providers**

Organizations in sectors such as transportation, energy, healthcare, and finance turn to telos for solutions that secure their operations and ensure compliance with industry-specific regulations. It’s important to protect critical infrastructure, it should be the priority in today’s security landscape.

**Commercial enterprises**

Telos collaborates with an extensive array of commercial businesses, ranging from large corporations to small and medium-sized enterprises. These organizations seek telos’ expertise in cybersecurity, risk management, and compliance to shield their operations and data.

**Defense and Military Organizations**

Telos has a robust history of collaboration with DoD and military entities, delivering solutions designed to address the distinctive security challenges inherent in their operations.

**Noteworthy Achievements**

Telos Corporation has earned a host of accolades and certifications, signifying its unwavering commitment to providing secure and compliant solutions. A prominent achievement is its accreditation as a FedRAMP-accredited Third-Party Assessment Organization (3PAO), underscoring its dedication to ensuring secure and compliant solutions, particularly within the government sectors.

**Initial Orientation and Training**

Before I started working with the content management team I was introduced to Olive. After we talked, she told me that we were going to have three meetings and each of those meetings would talk about different things. In the first meeting we held we got to know each other, and we talked about things we liked and current events. She then explained what the content management team does for Telos. While we held this meeting, I was waiting for one of the other departments to get my computer ready. They have special work on computers, and they want to ensure that it is safe to use and that it is programmed for me to have access to certain information. After the meeting ended, I got my computer, and I already had my username and password since I was working for the facilities department. I got to leave early on my first three days, however, I was told the total hours Telos employees must reach is 8 hours. The max is 8 hours, and you can't work over that. At the next meeting, we talked more about the management team and telos in general as I discussed previously on page 3. After the meeting, I was working on a couple of training assignments. Every Telos employee must complete their training and we get reminded by our security team to complete them. These repetitive training exercises will help mitigate risks. On my final days of meeting up with Olive, she told me more about the people who are on our team, and she introduced me to my first project. This meeting was held on a Wednesday and this day when we hold our weekly meeting with the rest of the team. I was introduced to the management team, which is composed of highly skilled and dedicated professionals with a shared passion for cybersecurity. The structured approach to content development and the meticulous attention to detail were among the initial impressions that left a significant impact. I realize that Telos places a high premium on producing accurate and high-quality content, which resonated with my aspirations as a content creator. I was surprised when I first started my project, it felt like I was doing a homework assignment with the answers right in front of me. It was more like an organization project rather than a critical thinking project. These projects that I first started on did not have anything linked to it, they were practice assignments that covered everything they did. Eventually, I started working on real projects after I got familiar with how things operate.

**Management**

Olive is my main manager at Telos. She described the management for telos as flat and not too intricate. For instance, other organizations' managers are usually administrative, and they must do things that help support higher authority. In most cases, some employees can have up to more than 4 managers. Telos is not like that and that is why my manager describes it as flat. There are only two managers in my field and it's Olive and my stepfather who are both our bosses. She does more than just administrative tasks, she helps by also working on tasks that we work on as well. I report everything I do to her, and she is the one who assigns me my projects. Other people in Telos can also be considered my boss since I'm just an intern but I don’t work for their department.

**Major work duties**

I had the pleasure of working on multiple projects in my time as an intern. I worked on mapping assignments, created content, Q&A, parsed projects, and managed overlays. As I stated earlier, I started working on practice assignments and they were there to teach me some of the things the management team does. My training week ended, and I got a real project.

**Mapping**

Tim is one of the guys in my management team who works primarily on mapping assignments. My manager Olive asked him to provide me with one of his tasks. We held a meeting and he explained to me what he wanted me to do. He gave me a list of NIST controls, and my objective was to create a mapping diagram. This diagram illustrates the relationships between different security controls within a selected control set, specifically those belonging to the Cybersecurity Framework (CSF). The controls are organized into subcategories, and the links between them represent controls that appear in the same CSF subcategory. For example, I used a lucid chart to create my diagram, and control AC-1 PE-2 are linked together. AC-4 might be linked to AC-1 but not to PE-2 and I must illustrate that in my diagram. There are over a thousand NIST controls and having that as my first task was a lot of work. It wasn’t due for a while, and I got Tim started so in the end I did help him before things got messy. Below is an image of his completed diagram.

A screenshot of a computer screen

Description automatically generated

The low baseline icon is an essential feature. Controls are categorized by impact levels; these levels are known as High medium and Low. Organizations don’t need a whole list of NIST controls. So, it’s important to group these controls by levels of importance. Some organizations need higher-level controls to help manage potential risks. For example, let’s compare a marketing business to a cleaning business. Both organizations have their employees sign up on a computer. One of the security control policies talks about login attempts the marketing team might only allow 3 attempts, while the cleaning service organization might allow 5+ attempts. This shows that the marketing organization has a higher baseline than the cleaning service.

**Q/A**

There are two sides to the content management team. One side is the developer side, and the other is Q/A. The developers are developing content that customers need. The Q&A side's objective is to check the work the developers did. I remember in Highschool we had moments where we would take a quiz and switch papers with our classmates to grade. The Q&A is just like that but different. For example, my manager Olive was working on an overlay assignment. Her objective is to extract controls from the ODP regulation into an Excel spreadsheet. Once she finished with her task, she sent it to me to check. I used a PDF that shows me what should be included.

I created another Excel sheet and at the top, it is labeled Q/A, Date, Error Type, ID, Project, Component field, Q/A notes, and resolution. Under Q/A I must indicate I was the one that checked it, Q/A can have more than one person checking. Under the date column, I should indicate when I found an error in her work. The next row at the top is the error type, this is where I would indicate what type of error it was. For example, it can be a source mismatch, possible typo, Content error, etc. Under the ID column, I must indicate what control had the error. This will help my manager know where the error occurred when she goes back in to make edits. The project Colom doesn’t change it’s the same for every mistake, it just indicates the name of the project. The component field also doesn’t change much, this just helps the developer know where to find this issue on Xcaxta360. Under the QA notes column, I would put her default answer and the correct statement that’s stated in the PDF. I would leave a note and explain what she did wrong. When working with regulations, it’s important to copy exactly what it says, we cannot make changes to government regulation. The management team's objective is to manage the controls, altering these controls can lead to consequences and issues. The final column labeled at the top of the spreadsheet is resolution. In this column, I would label l it as not fixed after checking Olive's work. When she fixes her errors and sends them back to me to check again, she would have labeled that column as fixed. Below is an image of a spreadsheet I created to show how I do Q&A for telos.

A screenshot of a computer

Description automatically generated

**OVERLAYS**

Managing overlays is an important task for the content management team. As I stated previously organizations don’t need every control that is listed in a regulation. Overlays show us which control an organization needs. I got assigned to work on intelligence overlays and there are three groups: INT-A, INT-B, and INT-C. My objective is to extract the correct controls for each group, and I put them in separate spreadsheets. The PDF will tell me where each of the security control policies goes. For example, the PDF will tell me that Access Control One (AC-1) should be included in both INT-A and INT-B but not INC-C. My job is to ensure that I read the passage correctly, so I don’t put a policy down for the wrong overlay group.

**Parsing Assignments**

Parsing assignments is something every developer must do for the most part. It’s the extraction process of security controls from government regulations. Some government regulations update their security controls and it's important that we also update our spreadsheets. For my parsing assignment, I was tasked with extracting controls from the regulation CSF. There was an update, and the new CSF is called CSF2.0. My objective was to develop a spreadsheet that compared both regulations. After I put it together in a spreadsheet, you can see which security controls stayed the same, which security controls got removed, and which security controls got added.

**Knowledge Check**

Before I began my internship, I only knew the basic terminology of cybersecurity. I knew that cybersecurity protected private information from hackers. There was a lot I did not know and as I stated earlier, I began my internship a couple of years ago. I started learning about cybersecurity from my internship, and after the summer ended, I started taking more cybersecurity classes in my junior year. Things started making sense to me because I was making connections between what I do at work with my schoolwork. For instance, my risk magnet class talks about how organizations manage and maintain risks. My internship already prepared me for this class, that’s what I've been doing year-round. My internship has helped me figure out what I wanted to do with cybersecurity. Before my internship, I didn’t know what field I wanted to get into. There’s IT, cloud security, application management, and many more. This internship helped me figure out what I liked to do.

**Internship goal**

I’ve been working as an intern for a while now and I got to learn a lot. I was nervous at first because didn't know what I was getting myself into. After a couple of weeks in the office, I was comfortable. There are a multitude of things that I enjoyed. For instance, I like how I get to work at my own pace. The projects I get have a due date, it’s like doing a homework assignment. I also really enjoyed teleworking; it was so convenient to be able to do work from home. There were some discouraging moments, but it wasn’t too serious. For example, I did not like that I had to work every day for 8 hours. I was okay at first, but it started weighing on me after a while. I’ve also had moments when I had a challenging assignment. Most regulations will have over 500 security controls, and I’ve had tasks that required I check 3 different regulations at the same time. So, in total, I would have worked with over 1,000 security controls. It was overwhelming and remembering the instructions started getting challenging.

Eventually, I got used to it and it got to a point when I stopped making mistakes. I would recommend future interns to listen, be observant, and ask questions. I learned a lot by asking questions, every time I got stuck on something I would my manager. Listening is key for this internship; my manager does a really good job of explaining my tasks to me. When working with a team it’s also good to be observant in meetings. One thing I’ve noticed is that the projects we work on are all connected in a certain way. We work as a team to handle a multitude of cybersecurity tasks.

**Conclusion**

Interning with the Telos content development team has been an enriching and transformative experience, providing valuable insights into the dynamic world of cybersecurity content creation. I learned more about cybersecurity and how this discipline protects me and everyone else who uses technology. Telos also helped me with a multitude of school assignments. I would use examples from work whenever I have a writing assignment that talks about cybersecurity. This internship helped me figure out what I liked about cybersecurity, if I was to apply for another job it would be for the content development team. I’ve gained a lot of experience and I hope to use what I’ve learned in the future.

**Citation**

1. Tools, C. (2022, March 27). *Co-occurrence network of security controls - CSF tools*. CSF Tools - The Cybersecurity Framework for Humans. <https://csf.tools/visualizations/csf-node-link-diagram-control-relationships/>
2. Telos Corporation. (2023, Steptember 12. Cyber Risk Management Platform: Compliance Automation: Xacta. <https://www.telos.com/offerings/xacta/>
3. Loudoun Economic Development. (2021, February 3). Telos, FBI Partner for Cybersecurity Training. Loudoun County Economic Development. https://biz.loudoun.gov/2021/02/03/telos-fbi-cybersecurity/