Final Internship Paper

Keller Beacham

TQI Solutions Inc.

Mid-Atlantic Regional Maintenance Center (MARMC)

SharePoint Specialist

Professor Teresa Duvall

CYSE 368 / Internship

Spring 2026

April 17, 2026

Table of Contents

1. Introduction

I decided to complete my internship with TQI Solutions Inc. at the Mid-Atlantic Regional Maintenance Center (MARMC) because it gave me the chance to work in a real operational environment that connects directly to both information technology and cybersecurity. As a Cybersecurity student at Old Dominion University, I wanted more than classroom knowledge. I wanted an internship where I could see how enterprise systems are actually managed, how users depend on those systems every day, and how security principles are applied in a workplace that supports important operations. The SharePoint Specialist position stood out to me because it involved access control, information management, data organization, and support for a large command. Those areas matched my long-term interests in cybersecurity, systems administration, and secure information handling.

Another reason I chose this internship was because it allowed me to build on skills I had already started developing through school, military experience, and previous IT support work. Before beginning this internship, I had experience helping users with technical issues and working in structured environments where accountability matters. I believed this internship would allow me to take those skills into a more advanced setting and use them in a role where the impact of my work would be visible. I also saw this opportunity as a way to strengthen my resume before graduation and to gain practical experience with Microsoft enterprise tools that many organizations use.

My internship took place through TQI Solutions Inc. while supporting MARMC in Norfolk, Virginia. MARMC is a large naval maintenance command, so the systems used there must support a wide range of users, departments, and mission needs. A large part of the organization’s work depends on reliable access to information, organized digital workspaces, and

secure data handling. SharePoint is important in that environment because it functions as a central platform for communication, storage, collaboration, and workflow support. Working in this setting gave me exposure to a professional environment where technology is not separate from operations. Instead, technology directly supports the day-to-day mission of the command.

At the beginning of the internship, I also had to complete orientation and role-specific training. Early on, I passed the Flank Speed NAVSEA Level 1 Site Collection Admin test and completed the required Site Collection Administrator Controlled Unclassified Information handling class. These initial requirements helped establish the expectations for the position and showed me that security and compliance were treated seriously from the beginning. My first impressions of the internship were that the role involved much more than just webpage updates. I quickly realized that maintaining SharePoint in a command environment requires attention to permissions, access rosters, content quality, user support, and governance standards.

My signed Memorandum of Agreement identified four learning objectives for the internship: safeguarding Personally Identifiable Information and Controlled Unclassified Information, learning Power BI basics, website and subsite development, and implementing reports and applications into SharePoint for user utilization. These objectives gave me a clear set of goals to work toward throughout the semester. They also fit well with my academic background because they combined cybersecurity, information systems, and real-world problem solving. Going into the internship, I hoped not only to meet those objectives but also to gain a better understanding of how technical work supports a large organization in practice.

Overall, I chose this internship because it was relevant to my degree, offered hands-on experience in a professional environment, and gave me the chance to work in an area that connects system administration, cybersecurity, and user support. From the beginning, I viewed the

internship as an opportunity to test what I had learned in school, grow in areas where I lacked experience, and prepare for a future career in cybersecurity and enterprise IT. By the end of the internship, it became clear that the experience gave me a much deeper understanding of how technology, governance, and security all come together in the workplace.

2. Management Environment at the Internship

The management environment at my internship was structured, professional, and strongly focused on accountability. Because the internship took place in support of a large naval command, there was a clear chain of responsibility and a strong expectation that work had to be accurate, organized, and completed in a timely manner. My supervisor, Dominique VanGundy, provided guidance on priorities and expectations while also allowing me to take ownership of different tasks as I became more capable in the role. That structure was helpful for me because it gave me a framework to learn within while still pushing me to become more independent over time.

One thing that stood out to me about the management environment was that work was not random. There were clear priorities tied to command needs, user requirements, and ongoing projects. Some tasks were reactive, such as handling tickets, resolving access issues, and responding to user concerns. Other tasks were proactive, such as cleaning up permissions, maintaining site content, preparing for audits, or helping improve reporting tools. This balance taught me that enterprise IT work requires both technical responsiveness and long-term planning. You cannot simply wait for problems to happen. You also have to maintain systems in a way that prevents problems before they start.

Communication was also an important part of the management environment. In my role, I interacted with content managers, end users, and other members of the SharePoint team. At times I had to explain technical issues in simple terms, especially when helping people understand permissions, access processes, or how SharePoint tools could be used more effectively. I also had to communicate with team members when working on larger efforts such as the post-migration quality analysis and PMS Viewer access control. These interactions showed me that technical

knowledge alone is not enough in a professional setting. To be effective, you also need to communicate clearly and work well with others.

The environment also emphasized standards and consistency. For example, part of my role involved making pages on the MARMC home site look more uniform in display, keeping information current, and maintaining control over access rosters. That kind of work may sound simple at first, but in a large organization consistency matters because many people rely on the same systems. A page that is disorganized, outdated, or inconsistent can create confusion and reduce trust in the system. Through this internship, I learned that management values not only technical functionality but also usability, professionalism, and reliability.

Another major aspect of the management environment was security awareness. Since MARMC works with sensitive operational information, there was a strong emphasis on controlling access, safeguarding data, and staying prepared for audits. My responsibility for the recurring 90-day PII audit made this especially clear. The management environment did not treat cybersecurity as something separate from daily work. Instead, security was built into routine responsibilities, such as checking permissions, cleaning up sites, reviewing stored content, and ensuring that users had the right access for the right reasons.

Overall, I would describe the management environment as effective for an internship because it combined oversight with real responsibility. I was not simply observing or doing busy work. I was trusted with tasks that mattered to the command, and I had to learn how to complete them in a way that met real organizational expectations. That experience helped me grow professionally and gave me a clearer understanding of what effective management looks like in an enterprise IT setting.

3. Major Work Duties, Assignments, and Projects

My major work duties as a SharePoint Specialist centered on maintaining the MARMC SharePoint environment and supporting the users who depend on it. A large part of my day-to-day work involved cleaning up permissions, maintaining the display of the MARMC home site and its subpages, making sure information was up to date, and verifying that pages looked professional and functioned correctly. This work required attention to detail because even small mistakes in a page, a broken link, or a permissions issue could affect a large number of users. Over time I also worked to make page displays more uniform, which helped improve the appearance and consistency of the main site.

Another one of my major responsibilities involved supporting and following up on the command's large shared drive to SharePoint migration. Before and during the migration, I helped classify data in the share drives, create folders and structure in SharePoint, and sort information so it could be moved in an organized way. Once the migration progressed, the work shifted toward quality assurance, cleanup, and user support. The SharePoint team migrated more than 3,239 gigabytes of data, which meant there were many follow-up issues involving access requests, missing data, misplaced files, and user errors. Supporting this process helped me see how large and complicated data migrations can be in a real organization.

I also worked on website and subsite development, which was one of the learning objectives identified in my internship agreement. Early in my time in the role, I started creating pages for military resources such as CMEO, SAPR, DAPA, FAP, and SCP. I also worked on other sites and subpages, including pages for areas like Manpower and Cybersecurity, and I helped edit multiple existing sites when information or layout needed to be improved. This part of the internship helped me understand that site development is not just about how a page looks. It is also

about how well information is organized, whether users can find what they need, and whether the page serves its purpose in a professional environment.

Ticket support was another major part of my work. Across different months I handled a steady number of tickets related to SharePoint needs, user issues, and access requests. In some months the ticket count was low because much of the work tied to the migration had to bypass the standard ticketing process due to urgency and volume. In later months, the ticket count rose significantly, including fifty-seven tickets in January and twenty-three in February. Handling tickets taught me how to manage user support in an environment where people may have very different levels of technical knowledge but still need timely help to continue doing their jobs.

One of the most important assignments I worked on involved access management for PMS Viewer. After the large data migration, a major portion of my responsibilities involved helping users get the access they needed to continue their work. Tyler Johnson and I were responsible for access control for many users in areas such as C200 and C900, and we also handled requests coming from outside commands. By February, we had dealt with more than two hundred requests for PMS Viewer access. This project showed me that access management is both a technical and an administrative responsibility. It requires accuracy, organization, and an understanding of why the access matters to the user and the command.

I was also assigned responsibility for the recurring 90-day PII audit in SharePoint, which was submitted to PEO Digital. This required me to review site areas, audit the Shared Area and the PII site, and make sure that exposed sensitive information was not being left in areas where it did not belong. Because a new audit was always approaching, this assignment pushed me to think beyond one-time fixes and instead focus on keeping the environment continuously ready for

review. The audit responsibility was one of the clearest examples of how my work contributed directly to governance and information security.

Finally, I began working with Power BI and started learning Power Apps. In Power BI, I created a gains-and-losses spreadsheet for civilians and contractors and turned that data into a dashboard that could be displayed on the MARMC main site. I also began helping create a SharePoint page and Power BI solution that would help new users track where they were in the onboarding process. These projects expanded my role beyond maintenance and support. They showed me that my internship also involved improving visibility, creating better tools for users, and thinking about how information can be presented in a way that supports decision making.

4. Use of Cybersecurity Skills and Knowledge in the Internship

Although my internship title was SharePoint Specialist, the work involved many cybersecurity-related skills and concepts. One of the strongest connections was access control. In cybersecurity classes, I learned that one of the most important principles in protecting systems and data is making sure users only have access to what they are authorized to use. At MARMC, that principle was part of my work almost every day. Whether I was managing permissions on SharePoint pages, controlling access rosters, or helping process PMS Viewer access requests, I was applying the same access control concepts that are discussed in cybersecurity courses.

Another major cybersecurity connection was the protection of sensitive information, especially Personally Identifiable Information and Controlled Unclassified Information. My internship agreement specifically listed safeguarding PII and CUI as a learning objective, and my work gave me direct exposure to why that objective matters. Being placed in charge of recurring PII audits made me more aware of how easy it is for data to become exposed if systems are not managed carefully. It also showed me that security is often about routine prevention rather than dramatic incidents. Many cybersecurity problems can begin with small mistakes such as incorrect permissions, poor file placement, or lack of monitoring.

My internship also strengthened my understanding of governance and compliance. In school, those ideas can sometimes feel abstract because they are discussed through policy, frameworks, or case studies. At MARMC, I could see how governance works in practice. There were expectations for how sites should be maintained, how permissions should be controlled, how information should be reviewed, and how audit readiness should be maintained. The 90-day PII

audits were a strong example of compliance in action because they required systematic review and accountability. This helped me understand that cybersecurity is not just technical defense. It also involves process, documentation, and the ability to prove that systems are being managed responsibly.

I also used problem-solving skills that connect directly to cybersecurity work. During the shared drive to SharePoint migration and the long period of post-migration cleanup, I regularly dealt with access issues, misplaced information, user errors, and questions from people trying to find what they needed. Those situations required me to investigate the problem, determine what was causing it, and apply a solution without creating new issues somewhere else. That type of step-by-step analysis is similar to the thinking used in cybersecurity when evaluating incidents, vulnerabilities, or system misconfigurations.

Another way cybersecurity knowledge appeared in the internship was through secure system administration. A secure environment does not happen automatically. It has to be maintained through regular review, correct permissions, standardized practices, and careful change management. My work maintaining SharePoint pages, cleaning up displays, organizing document libraries, and teaching content managers how to use the tools available to them all supported a safer and more reliable environment. Even though these tasks may not look like traditional security operations, they still contribute to security by reducing confusion, limiting mistakes, and supporting proper information handling.

My experience in the internship changed my understanding of cybersecurity by showing me how often security is embedded into regular IT responsibilities. Before this internship, I often thought of cybersecurity in terms of threats, attacks, and defensive tools. Those topics are still important, but this role taught me that cybersecurity also lives in everyday work like permissions

management, data reviews, governance processes, access requests, and user education. In other words, cybersecurity is not always separate from IT operations. In many workplaces, it is built into how systems are maintained and how information is controlled.

Overall, the internship helped me connect classroom cybersecurity knowledge to the real world in a way that was much more practical and specific. I was able to apply concepts I already knew, such as access control and information protection, while also learning how those concepts work inside an enterprise environment where users, leadership, and operational needs all have to be considered. That made the subject matter feel more concrete and more relevant to the kind of work I want to pursue after graduation.

5. How the ODU Curriculum Prepared Me for the Internship

The curriculum at Old Dominion University helped prepare me for this internship in several important ways, even though the internship also exposed areas where classroom learning can only go so far. My cybersecurity coursework gave me a foundation in security principles, information assurance, risk awareness, networking, and system concepts that directly supported my ability to understand the work I was doing at MARMC. Because of those classes, I already had a basic understanding of why permissions matter, why sensitive information must be handled carefully, and why system organization and accountability are important in a secure environment.

One of the strongest ways ODU prepared me was by helping me think analytically about technical problems. In class, many assignments require students to break down an issue, examine different parts of a system, and think carefully before applying a solution. That mindset translated well into my internship, especially during the post-migration cleanup and user support work. When users had missing access, when site content needed to be reorganized, or when I had to review areas for possible PII exposure, I had to work through those issues in a structured way. My coursework helped me feel comfortable approaching technical tasks step by step instead of guessing.

My cybersecurity classes also helped me recognize the importance of least privilege, data confidentiality, and risk reduction. Even if those ideas were often introduced in class through theory, frameworks, or lab exercises, the internship gave me a chance to see them in a live environment. For example, when helping manage access for SharePoint or PMS Viewer, I was not simply completing an administrative task. I was helping make sure that access aligned with job

needs and organizational requirements. Because of my academic background, I already understood why those controls matter.

In addition, ODU prepared me through writing and communication assignments. Throughout the cybersecurity program, I have had to explain technical ideas in papers, discussions, and project work. That experience helped me during the internship because I often needed to communicate clearly with users, content managers, or team members who might not all have the same technical background. Being able to explain a problem, describe a process, or document work clearly is important in both school and the workplace. The internship reinforced that strong communication is a necessary professional skill, not just an academic one.

At the same time, the internship showed me some areas where school can only prepare you partially. For example, I had not previously worked deeply with SharePoint administration, Power BI, or Power Apps in my courses. I also had limited exposure to the specific workflows, standards, and user expectations that come with supporting a large government command. Classroom learning can teach concepts and provide controlled practice, but the workplace introduces complexity that is harder to simulate. Users have real deadlines, systems already exist before you arrive, and problems are not always clearly defined. That is where the internship filled in the gap between theory and practice.

The internship also revealed new concepts and techniques that I had not yet encountered in the classroom. One example was the recurring PII audit process and the level of detail required to keep an environment ready for audit. Another example was the practical use of business intelligence tools to present workforce data and support onboarding processes. Learning how Power BI dashboards can support leadership and how SharePoint can be used for workflow visibility expanded my view of what IT and cybersecurity-related work can include.

Overall, I would say ODU prepared me well in terms of foundational knowledge, problem-solving habits, and professional communication, but the internship added the real-world experience needed to make those lessons fully meaningful. The combination of school and internship experience has been valuable because the classroom gave me the base, and the internship showed me how to use that base in an actual enterprise setting.

6. Learning Outcomes and Whether the Internship Met Them

My internship agreement identified four primary learning objectives: safeguarding PII and CUI, learning Power BI basics, website and subsite development, and implementing reports and applications into SharePoint for user utilization. Looking back on the internship, I believe the experience met all four objectives, although some were developed more deeply than others. The value of the internship is that it did not just expose me to these topics once. Instead, it gave me repeated opportunities to apply them in real situations.

The first objective was safeguarding PII and CUI. I believe this outcome was strongly met. From the beginning of the internship, security and proper information handling were clearly important. I passed required training related to Site Collection Administration and CUI handling, and later I became responsible for the recurring 90-day PII audits for SharePoint. Reviewing sites for possible leaks, auditing the Shared Area and PII site, and working to keep the environment ready for inspection gave me real experience with data protection responsibilities. This objective was especially important because it connected directly to cybersecurity and showed me how governance and information protection work in practice.

The second objective was learning Power BI basics. This objective was also met. During the internship, I began working with Power BI and learned how to take data from a gains-and-losses spreadsheet and turn it into a dashboard that could be displayed on the MARMC main site. I also started participating in a Power BI and SharePoint solution related to onboarding. While I would not say I became an expert in Power BI during the internship, I definitely built a solid beginner foundation and developed confidence using the tool in a work environment.

The third objective was website and subsite development. This objective was met throughout the internship because site work was one of the most consistent parts of my responsibilities. I maintained the MARMC home site and subpages, worked to keep content current, improved layout consistency, created and edited pages for different areas, and helped make the SharePoint environment more professional and usable. This objective gave me direct experience with how websites and subsites function in an enterprise environment where organization, permissions, and presentation all matter.

The fourth objective was implementing reports and applications into SharePoint for user utilization. This objective was partially connected to my Power BI work and also to my growing exposure to Power Apps. The gains-and-losses reporting project clearly supported this learning objective because it involved creating data displays that users and leadership could access through SharePoint. The onboarding tracker project also supported this objective because it was designed to improve user visibility during a process that can otherwise be difficult to track. My learning in Power Apps was still in the earlier stages, but the internship definitely moved me in the right direction and helped me understand how these tools can work together within SharePoint.

In addition to the official learning objectives, the internship also helped me achieve outcomes that were not stated as directly in the agreement. For example, I became much stronger in access management, user support, audit readiness, and enterprise information governance. I also became more comfortable working in a professional environment where systems affect a large number of users and where mistakes can have wider consequences. Those lessons were just as important as the technical objectives because they helped me mature professionally.

Overall, I can say that the internship fulfilled its intended goals. Some objectives, such as website development and data protection, became major parts of my regular responsibilities.

Others, such as Power BI and Power Apps, developed later in the internship but still gave me meaningful growth. Most importantly, the experience gave me practical understanding instead of just theoretical exposure. That is what made the learning outcomes feel real and valuable.

7. Most Motivating or Exciting Aspects of the Internship

The most motivating aspect of this internship was knowing that my work supported a real organization and had a direct impact on the people using the systems. In many school projects, the assignment ends when the grade is submitted. At MARMC, the work mattered beyond that. If a page was not maintained correctly, if access was delayed, or if information was hard to find, it affected real users who depended on the system to do their jobs. That made the work feel more meaningful and kept me motivated to take it seriously.

Another exciting part of the internship was being trusted with responsibilities that grew over time. I did not stay limited to one type of task. As the internship continued, I gained exposure to more advanced responsibilities such as the 90-day PII audits, PMS Viewer access control, Power BI projects, and broader site maintenance. Being trusted with those responsibilities showed me that I was progressing and that my role had value. It was motivating to see that I was not only learning but also contributing in ways that mattered to the command.

I was also motivated by the connection between the internship and my future career goals. Because I want to work in cybersecurity, it was exciting to see how many security-related ideas were present in the role even though the position focused on SharePoint. Managing permissions, protecting sensitive information, reviewing sites for PII exposure, and supporting audit readiness all gave me relevant experience. The internship helped me realize that cybersecurity careers do not always begin in a role labeled “cybersecurity.” Sometimes the best experience comes from positions where security is built into the daily work.

Learning new tools was another exciting part of the experience. Working with SharePoint at an enterprise level was already valuable, but getting the chance to use Power BI and begin learning Power Apps added another layer of interest. I enjoyed seeing how data could be

transformed into dashboards and how those dashboards could improve visibility for leadership or users. The onboarding tracker project was especially interesting because it focused on improving the user experience rather than only maintaining existing systems.

I was also motivated by the professional growth that came with the internship. The role required patience, communication, organization, and consistency. It pushed me to be more detail-oriented and more careful about how I approached technical tasks. It also made me more confident in my ability to work in a professional setting, interact with users, and contribute to projects that support a large organization.

Overall, the most exciting part of the internship was the combination of learning and real responsibility. I was able to develop technical skills, apply concepts from school, and see how my work fit into a larger operational environment. That combination made the experience more motivating than a typical classroom assignment and gave me a clearer sense of the kind of work I want to continue pursuing.

8. Most Discouraging Aspects of the Internship

Although my internship was very valuable overall, there were still discouraging aspects of the experience. One of the most discouraging parts was how time-consuming and repetitive some of the work could become, especially during the long period of post-migration cleanup. After a large migration, there were many issues involving access, misplaced files, missing data, and user confusion. A lot of that work was necessary, but it could also feel repetitive because many problems were similar and required careful review before they could be resolved.

Another discouraging aspect was seeing how easily users can become frustrated when systems change. The move from shared drives to SharePoint affected a large number of people, and not everyone adjusted to the new environment at the same pace. Some users had trouble finding files, some needed new permissions, and others were dealing with unfamiliar processes. As someone supporting those users, I learned that technical improvements do not always feel like improvements to the people affected right away. That was sometimes discouraging because even when the team was making progress, users were still dealing with disruption.

It could also be discouraging when access issues or permissions requests involved delays outside of my direct control. In a structured environment, not every problem can be solved instantly. Some requests require review, coordination, or confirmation before action can be taken. That taught me patience, but it was still difficult at times because I wanted to help users more quickly. It showed me that in real workplace settings, technical ability is important, but workflow and process constraints also shape what can be done.

Another discouraging part of the internship was realizing how much small errors can matter in enterprise environments. Something as simple as a wrong permission, an overlooked document, or inconsistent site content can create larger issues for users or compliance. That level of

responsibility is important, but it also adds pressure. There were times when I felt the weight of needing to be extremely careful because mistakes could affect more than just me.

Finally, one discouraging realization was that some learning has to happen slowly. I wanted to become more advanced in tools like Power BI and Power Apps as quickly as possible, but in a professional environment you still have to balance learning with the daily responsibilities of the job. That means progress in new areas can sometimes feel slower than you want. Even so, I came to understand that steady growth in a real workplace is more valuable than rushing through concepts without truly understanding them.

Overall, the discouraging aspects of the internship were not enough to take away from the value of the experience. Instead, they showed me the more difficult side of enterprise IT work, including repetition, user frustration, delays, and the pressure of accuracy. Those challenges were important because they gave me a realistic picture of the field rather than only showing me the interesting parts.

9. Most Challenging Aspects of the Internship

The most challenging aspect of the internship was managing the complexity that comes with supporting a large organization. MARMC is not a small office with a limited number of users and simple workflows. It is a large command with many departments, many users, and a strong need for organized, secure information systems. Because of that, even basic tasks could become more challenging than expected. A single permissions issue might involve multiple users, different site areas, and follow-up questions about what access is actually needed. That complexity forced me to slow down, pay attention, and avoid making assumptions.

The shared drive to SharePoint migration and the long period of cleanup after it were also very challenging. Large amounts of data had to be classified, structured, migrated, and then reviewed after the move. Once the migration was complete, the challenge shifted from moving data to helping users adjust to the new environment and resolving the problems that followed. This included dealing with access requests, lost or misplaced files, document library organization, and user errors. The challenging part was not only the volume of the work but also the fact that the issues were interconnected. Fixing one problem often required understanding the bigger structure of the environment.

Another major challenge was managing access control accurately. When working with permissions on SharePoint or handling PMS Viewer requests, I had to be careful because granting the wrong access could create security issues while denying necessary access could interrupt operations. That balance between security and usability is one of the most important lessons I took from the internship. It is easy to talk about access control in theory, but in practice it requires judgment, attention to detail, and accountability.

The recurring PII audit process was also challenging because it required a preventive mindset. It was not enough to fix obvious issues after they were found. I had to think in terms of continuous readiness and look for potential problems before they could become audit findings or security concerns. Reviewing large areas for sensitive data takes concentration and patience, especially when the environment is active and always changing. This responsibility challenged me because it required consistent discipline rather than a one-time effort.

Learning new tools while still handling regular responsibilities added another challenge. As I started working with Power BI and learning Power Apps, I had to balance the need to learn with the need to continue supporting day-to-day operations. In the workplace, you do not always get to pause your regular duties in order to focus entirely on something new. That taught me how to learn incrementally, ask questions when needed, and build confidence over time instead of expecting to master everything immediately.

Overall, the challenges of the internship helped me grow the most. They pushed me to become more organized, more patient, and more thoughtful in how I approached technical work. The experience taught me that challenging work is often where the most learning happens, especially when the work matters and has real consequences for users and the organization.

10. Recommendations for Future Interns

Based on my experience, I would recommend that future interns in this role prepare in several ways before they begin. First, they should build a solid base in Microsoft 365 tools, especially SharePoint, because the internship moves much more smoothly when you already understand the basics of sites, pages, permissions, and document libraries. An intern does not need to know everything on day one, but having familiarity with the platform will make it easier to learn the more specific tasks required by the command.

Second, future interns should review cybersecurity concepts related to access control, data protection, and least privilege. Even if the position is not labeled purely as a cybersecurity role, those ideas come up often in the work. Permissions, PII handling, and user access requests are all easier to understand when you already know why security controls matter. Interns who come in with that mindset will likely adapt faster and make better decisions when helping with access and governance tasks.

Third, I would recommend that future interns improve their communication skills before starting. A lot of the work involves helping users, explaining processes, and interacting with content managers or teammates. Technical knowledge is important, but patience and clarity are just as important. Some users will not understand SharePoint well, and some issues may be frustrating for them. Being able to stay professional and explain things calmly makes a big difference.

I would also recommend that future interns be ready to work carefully with large amounts of information. In this role, details matter. A person who is careless with permissions, data placement, or documentation can create larger problems for the command. Interns should be

comfortable double-checking their work, staying organized, and asking questions when they are unsure. Accuracy matters more than speed in many parts of the job.

Another good preparation step would be learning basic Power BI concepts and becoming open to learning Power Apps or other related tools. As organizations use more dashboards, reporting, and workflow tools, these skills become increasingly valuable. Even a beginner understanding can help an intern contribute more quickly to projects involving reporting or process improvement.

Finally, I would tell future interns to come in with a willingness to learn from both the technical and professional sides of the job. This internship is not only about learning software. It is also about learning how to operate in a structured workplace, manage responsibilities, communicate well, and support real users. Interns who approach the experience seriously and stay open to feedback will get much more out of it. Overall, the best preparation is a combination of technical basics, professional attitude, and patience.

11. Conclusion

In conclusion, my internship as a SharePoint Specialist with TQI Solutions Inc. supporting MARMC was one of the most important professional experiences I have had during my college career. It gave me the chance to move beyond classroom assignments and work in an enterprise environment where technology directly supports a large organization. Through this internship, I developed stronger technical skills, gained real experience with permissions management, site maintenance, access control, PII auditing, Power BI, and user support, and learned how important governance and accountability are in day-to-day IT work.

One of the biggest takeaways from this internship is that cybersecurity and information technology are deeply connected. Before this experience, I already understood many cybersecurity concepts from school, but the internship showed me how those concepts appear in regular workplace responsibilities. Access control, sensitive data protection, audit readiness, and user education were all part of my daily work even though my title was not specifically a cybersecurity title. This experience helped me see that secure systems depend on consistent operational work, not just specialized security tasks.

The internship also helped me better understand my own strengths and areas for growth. I learned that I am comfortable working in structured environments, that I can support users patiently, and that I take data protection responsibilities seriously. At the same time, I also saw how much more there is to learn, especially with tools like Power BI and Power Apps and with the broader processes that support enterprise systems. That realization has motivated me rather than discouraged me because it confirmed that this is a field where continuous learning is necessary.

This internship experience will influence the remainder of my time at ODU by giving me more purpose in my coursework. When I study cybersecurity topics now, I can connect them more directly to situations I have seen in the workplace. That makes the material feel more real and helps me understand why it matters. It also gives me a stronger foundation for future classes, projects, and conversations about professional goals.

Most importantly, this internship will influence my future professional path by reinforcing my interest in cybersecurity, enterprise IT, and information systems management. I want to continue developing in roles where I can combine technical skill, security awareness, and user support. The internship showed me that I enjoy work that involves both problem-solving and responsibility, and it gave me confidence that I can contribute effectively in professional environments. Overall, the experience was meaningful not only because of the tasks I completed but because of how much it shaped my understanding of the career path I want to pursue.