CYSE 368 Internship Final Paper

Old Dominion University

SSI /Aegis-TechRep

Mohammed Aljuboor

11/23/2024

Table of Contents:

1- Introduction:

In the ever-changing sector of cybersecurity, the ability to translate academic knowledge into practical, real-world solutions is critical to success. My internship during the CYSE 368 course gave an invaluable opportunity to bridge the gap between academic concepts and actual practices, notably in the area of system security. Throughout this internship, I worked in a variety of roles that needed a combination of technical knowledge, leadership skills, and a grasp of governance, risk, and compliance (GRC) frameworks. These experiences not only reinforced my previous skills, but also provided me with new ideas on system security within an organization.

This paper analyzes my internship experience in detail, concentrating on three key areas: technical duties, leadership and cooperation, and GRC. In the technical segment, I discuss my involvement in safeguarding systems, troubleshooting complicated issues, and streamlining processes to improve the organization's overall security posture. The leadership and collaboration section goes into my experience managing teams, developing good communication, and dealing with team dynamics in the workplace. Finally, the GRC section discusses how cybersecurity policies, regulatory compliance, and access control methods are crucial in maintaining system integrity.

This internship provided me with invaluable knowledge and abilities, which have helped shape my professional development. As I continue to concentrate in system security, I've gained significant knowledge about both the technical and organizational sides of cybersecurity. Reflecting on these experiences, I hope to provide a comprehensive account of my development as a system security professional, as well as how this internship prepared me for the challenges and opportunities that await me in safeguarding organizational systems and networks.

2- Main Section:

My work path has been purposefully centered on system security, with backing from both academic studies and several industry-recognized certifications. I am certified in Network+ and Security+, which have given me a thorough understanding of network management, system administration, and cybersecurity essentials. These certifications cover a wide range of topics, such as network configuration and management, troubleshooting, security protocols, risk management, and threat mitigation. These skills have been critical to my capacity to comprehend and address technological difficulties, as well as protect networks and systems from external and internal threats.

In addition to my technical credentials, I obtained a Governance, Risk, and Compliance (GRC) certification from Axure SC900. This certification has helped me understand how firms should link their cybersecurity strategies with larger governance and regulatory requirements. GRC frameworks are essential for ensuring that security policies, risk management strategies, and regulatory compliance initiatives are fully integrated into the organization's operational processes. By learning the fundamentals of GRC principles, I've gained a great grasp of the balance between security and compliance, appreciating the importance of protecting organizational systems while conforming to legal and regulatory norms.

Throughout my internship, I was able to apply my technical and theoretical knowledge to real-world cybersecurity concerns. I took on a variety of activities and responsibilities, from hands-on technical chores in system administration and network security to participating in collaborative, high-level conversations about organizational security posture and compliance. Each of these assignments enabled me to combine academic learning with practical skills,

enhancing my technical proficiency and broadening my understanding in crucial areas such as system security, leadership, and compliance.

I was able to troubleshoot and address a wide range of technical concerns, including system security, network administration, and infrastructure management. Whether it was resolving vulnerabilities, controlling firewalls, or improving system configurations, I used my qualifications and academic experience to find and execute successful solutions. My ability to address security concerns methodically and informed enabled me to make a meaningful contribution to the team and the organization as a whole.

My leadership obligations enhanced my professional talents. I got the opportunity to oversee a team of four employees, which gave me important lessons in delegating, mentorship, and dispute resolution. Balancing leadership responsibilities with technical tasks proved to be a constant challenge, but it gave me the opportunity to improve my communication and time management abilities. Through hands-on mentoring and team performance oversight, I got a better knowledge of team leadership dynamics, especially in a cybersecurity context where collaboration and efficiency are crucial.

Finally, my interaction with the Governance, Risk, and Compliance (GRC) team was an important aspect of the internship. I helped manage access control, ensuring that systems were protected by strong permissions and that users only had access to resources that were appropriate for their responsibilities. This experience helped me grasp how GRC principles overlap with security activities, resulting in a more comprehensive approach to protecting organizational assets. My experience reviewing compliance with internal policies and regulatory standards, as well as implementing the concept of least privilege, taught me the value of documentation, processes, and controls in maintaining secure environments.

I obtained a thorough understanding of system security by integrating my credentials, academic knowledge, and practical experience. The practical use of these abilities has not only increased my technical knowledge but has also improved my understanding of how cybersecurity fits into company policies and regulatory standards. This major section serves as a monument to my journey, showcasing how my qualifications, technical expertise, and hands-on experience have all contributed to my growth as a security professional.

A) Technical Responsibilities and Problem-Solving:

During my internship, I was in charge of various essential technical duties, including the management and security of crucial systems and networks. I helped improve the organization's security posture and overall system efficiency by leveraging my knowledge of tools and technologies such as Active Directory (AD), System Center Configuration Manager (SCCM), STIG, Multi-Factor Authentication (MFA), Mobile Device Management (MDM), Group Policy, firewalls, and Access Control Lists (ACL). Here's an outline of the specific places where I used my technical skills.

Active Directory (AD) was fundamental to my responsibilities for managing user identities and ensuring network access limits. I set up and maintained AD systems to ensure proper user account management, which included adding, changing, and deactivating accounts. I also put in place regulations to manage access to resources and group memberships, ensuring that sensitive material was only accessible to authorized personnel. In addition, I used Active

Directory to manage rights and enforce security policies across the network, helping to keep the IT environment secure and structured.

System Center Configuration Manager (SCCM) was crucial in organizing and deploying software updates and patches throughout the company. I used SCCM to automate the release of operating system updates, security patches, and software packages, ensuring that all computers were up to date and protected against vulnerabilities. Through SCCM, I was able to monitor system health, track compliance with security protocols, and automate the distribution of critical patches, thereby reducing the risk of security breaches caused by outdated software.

I actively collaborated with STIG to ensure that systems met the Department of Defense (DoD) security criteria. I helped improve the overall security posture of systems by implementing recommended configurations and settings to eliminate vulnerabilities. This entailed examining the security configuration of operating systems and applications, making any necessary changes, and documenting these changes to meet compliance requirements. My STIG experience assisted in ensuring that systems followed tight security rules, so helping to organizational compliance and risk mitigation.

Multi-Factor Authentication (MFA) was an important security precaution that I helped establish throughout the firm. I set up MFA to provide an extra layer of protection for accessing important systems and applications. By integrating MFA solutions with AD and other systems, I guaranteed that users had to submit several kinds of authentication (such as passwords and one-time passcodes) in order to acquire access. This dramatically reduced the danger of unwanted access caused by compromised credentials and improved overall network security.

Mobile device management has become increasingly important as remote work and mobile device usage have grown. I assisted in the implementation of a Mobile Device Management (MDM) system to protect the security of business data stored on mobile devices. I secured mobile devices that connected to the network from potential dangers by implementing security measures such as device encryption, remote wipe capabilities, and secure application management. MDM enabled centralized management of mobile devices, improving security and increasing productivity.

Group Policy was a valuable tool for enforcing security settings and configurations throughout the network. I used Group Policy Objects (GPOs) to standardize and automate system configurations like password policies, lockout policies, and user rights assignments. Through GPOs, I was able to implement security measures on a granular level across user accounts, computers, and organizational units. This centralized management enabled me to ensure consistent security configurations across the network, reducing administrative overhead while improving compliance with organizational security standards.

I also used firewalls and Access Control Lists (ACLs) to safeguard the network perimeter and manage access to network resources. I set up and monitored firewalls to prevent illegal traffic and protect against any external threats. In addition, I used ACLs on routers and switches to manage inbound and outbound traffic, ensuring that only authorized devices could access sensitive resources. By establishing suitable rules and policies in both firewalls and ACLs, I helped protect the network from both internal and external security vulnerabilities.

Through these technical responsibilities, I used a combination of my credentials and hands-on experience to resolve security issues, improve system performance, and guarantee that best practices were followed in all areas. My knowledge of AD, SCCM, STIG, MFA, MDM,

Group Policy, firewalls, and ACLs enabled me to address potential vulnerabilities and improve the overall security and functioning of the organization's IT infrastructure. Each of these roles improved my technical problem-solving abilities, allowing me to efficiently address complex security concerns.

B) Leadership and Collaboration:

In addition to my technical responsibilities, I spent a large portion of my internship honing my leadership abilities and improving my ability to interact effectively with cross-functional teams. As a Senior System Administrator, I had the ability to lead a small team, manage projects, and collaborate with other departments to achieve organizational goals. During these experiences, I improved my communication, delegating, and mentorship skills while also contributing to a collaborative and productive work environment.

A significant portion of my leadership experience included supervising a team of four individuals. This job gave me an invaluable opportunity to hone my skills in team coordination, task delegation, and performance management. I was in charge of monitoring daily operations, which included responding to support tickets in a timely and effective manner. I also ensured that team members had all of the resources and expertise they needed to fulfill their responsibilities. As a result, I had to prioritize work and assign assignments based on each team member's abilities and knowledge, guaranteeing an efficient workflow while upholding high standards of work.

My ability to manage priorities and mix technical tasks with leadership responsibilities was continuously questioned. I led by example, resolving technical difficulties as needed while also helping my team through complex scenarios. This combined role not only improved my leadership abilities, but also reinforced my grasp of the important balance between technical expertise and successful team management.

Collaboration was essential to my internship experience, as many of the activities I worked on required input and coordination with other departments. For example, when handling cybersecurity events or system setups, I frequently collaborated with the network and security teams. During these collaborative endeavors, I learnt the value of clear and succinct communication, particularly when dealing with critical concerns like system outages or security breaches. I attended daily stand-up meetings and debrief sessions, during which we exchanged updates, reviewed technical concerns, and verified that our approach to problem solving was consistent.

Working with cross-functional teams also provided me with a broader understanding of how different divisions inside the organization contribute to the overall security posture. I collaborated with members of the risk management, compliance, and governance teams to ensure that security protocols met internal policies and regulatory standards. These experiences not only improved my teamwork and problem-solving abilities, but also helped me realize the value of collaboration in driving corporate success.

Effective communication was crucial to both my leadership and collaborative activities. Whether I was mentoring a coworker, delivering updates to senior management, or working with other departments, effective communication was crucial. I improved my capacity to respond to support tickets in a succinct and informative manner, ensuring that both technical and non-

technical stakeholders could quickly understand the problem and solution. I also presented project updates and system enhancements to leadership, which helped me develop my public speaking and presentation abilities.

My ability to communicate complicated technological difficulties in a clear and intelligible manner was critical in overseeing cross-departmental initiatives and crises. I learnt how to adjust my communication style for varied audiences, whether it was discussing a technical issue to a non-technical manager or providing thorough technical documentation to the cybersecurity team.

Conflict is unavoidable in any leadership capacity, and during my internship, I was able to resolve minor team issues. These scenarios frequently emerged as a result of divergent perspectives on how to handle technical issues or prioritize activities. I attempted to arbitrate these situations by listening to all parties concerned, promoting open communication, and identifying common ground. By creating a positive and supportive environment, I was able to efficiently resolve issues, allowing the team to focus on its goals without disturbance.

Another important component of my leadership role was inspiring my team members. I made it a point to acknowledge their accomplishments, congratulate their victories, and offer constructive suggestions for growth. By creating a pleasant work atmosphere and exhibiting trust in their talents, I was able to keep the team motivated and focused on our shared objectives.

Overall, my leadership and cooperation experiences helped me get a comprehensive awareness of the workplace's technical and interpersonal components. I was able to fine-tune my leadership approach by combining technical expertise with great communication, mentoring, and

conflict resolution abilities. These experiences will continue to define my career as I aim to lead teams, manage difficult projects, and contribute to the success of future enterprises.

C) Governance, Risk, and Compliance (GRC):

During my internship, I worked closely with the Governance, Risk, and Compliance (GRC) team, gaining significant insights into the vital convergence of cybersecurity, organizational policy, and regulatory compliance. My primary responsibilities were managing access privileges, assuring adherence to legal and internal security laws, and assisting with attempts to meet specific Department of Defense (DoD) IT requirements, notably those related to information classification and security clearance.

My responsibility in GRC included supervising the organization's access control framework. This involved examining and changing user permissions to ensure that people only had access to the information they needed for their roles an important practice for adhering to the principle of least privilege.

Given the sensitivity of the data handled by the company, additional attention was paid to systems that required varied levels of security clearance. Security clearances are critical for ensuring the integrity of sensitive material, particularly in DoD environments. I worked with Secret and Top-Secret access levels, which are important variances in how information is handled by the government and defense sectors.

- **Secret clearance:** provides access to secret material that, if exposed, might have major consequences for national security. Personnel with Secret clearance are tasked with handling sensitive information that requires increased security but does not require the highest level of classification.
- **Top Secret clearance**: grants access to the highest classification of material, which, if exposed, might cause extremely serious harm to national security. This clearance is required for those who handle the most sensitive defense and intelligence data.

Understanding the significance of these clearance levels was crucial in ensuring that appropriate controls were installed, allowing only authorized workers access to classified documents, especially when managing access to DoD IT systems.

I worked with top security staff to ensure that users received access depending on their job function, role within the organization, and clearance level. This procedure included regular audits and reviews to assure compliance with DoD access control policies, which are crucial in preventing unauthorized access to classified systems and data.

One of the most important aspects of my internship was working inside the scope of DoD IT security standards. The Department of Defense imposes tough regulations and requirements to protect national security systems and keep sensitive data secure. These rules are especially important for those working in defense contracting or federal agencies, which frequently handle sensitive or classified information.

I helped build systems and processes that were meant to meet the National Institute of Standards and Technology (NIST) standards, which serve as the foundation for the Department

of Defense's cybersecurity requirements. These frameworks provide guidance on access control, security configuration, and incident response, all of which are critical for complying with federal and DoD regulations.

For example, ensuring that systems were set in accordance with Security Technical Implementation Guides (STIGs) aided in the enforcement of DoD standards for safeguarding operating systems, applications, and network components. By following these standards, I helped ensure that the IT environment satisfied the DoD's security requirements for handling secret material, particularly for Top Secret and Secret systems. In addition, I collaborated closely with the compliance team to identify and address vulnerabilities that could jeopardize the security of classified systems. By proactively identifying risks, I helped to reduce the chance of security breaches and ensured that sensitive data was protected in compliance with DoD security requirements.

The DoD's Risk Management Framework (RMF) is an important part of the GRC process in defense-related enterprises. The RMF offers a structured strategy to discovering, assessing, and reducing risks connected with information systems and security. During my internship, I worked on numerous stages of the RMF process, focusing on risk identification, assessment, and mitigation techniques.

I was responsible for conducting risk assessments to detect potential vulnerabilities and threats to organizational systems. This method entailed working with cross-functional teams to assess existing security controls and implement modifications as needed. Additionally, I helped document compliance with the RMF, ensuring that all security controls and risk mitigation strategies were properly implemented and aligned with the organizations overall security policies.

Through these activities, I gained a better knowledge of how organizations in sensitive industries like defense and national security work in highly regulated environments, balancing security requirements with operational needs. This experience has helped me better understand how to develop and manage cybersecurity controls inside frameworks such as the RMF to ensure legal and regulatory compliance.

A big problem in my employment was streamlining the process of managing user access changes, especially when there were position changes, department reorganizations, or other transitions that impacted access control. Working with the GRC team, I helped automate numerous areas of the access management process. This includes optimizing operations to ensure that security protocols were followed consistently and changes to access privileges were properly documented.

Automation played a critical role in decreasing errors, increasing efficiency, and ensuring that access changes were handled promptly. In addition, I assisted in the development and maintenance of thorough documentation, which is required for compliance and audits. This documentation not only served as a record of access changes, but it also facilitated more efficient audits and compliance checks.

One of the most important takeaways from my time at GRC was the need to strike a balance between security and usability. MFA, strict access control regulations, and clearance requirements are all necessary security measures for securing sensitive information. However, these measures also need to be implemented in a way that does not hinder the ability of employees to perform their work efficiently.

For example, while multi-factor authentication (MFA) is critical for improving security, it must be easily incorporated into the workflow to avoid delays or disrupting regular operations. Similarly, while strict access controls are required to protect classified material, ensuring that legitimate users have easy access to the resources they require is critical for maintaining productivity. Finding the right balance between strong security and operational efficiency is a key component of good governance, risk management, and compliance.

Overall, my time working in Governance, Risk, and Compliance (GRC) provided me with practical knowledge of how cybersecurity rules and regulatory frameworks, such as those employed by the DoD, affect day-to-day operations. By assisting with access privilege management, DoD IT compliance, and risk management processes, I was able to improve the organization's security posture while guaranteeing adherence to internal and external rules. This experience has given me a better knowledge of how governance and compliance are critical components of a holistic cybersecurity strategy.

3- Conclusion:

In conclusion, my internship experience has been transformative, allowing me to use theoretical information garnered from my studies in real-world circumstances. It has helped me to hone my technical skills, notably in system security, risk management, and governance. I am now more confident in my capacity to manage complex cybersecurity systems, lead teams, and maintain compliance with essential legislation.

Throughout my internship, I had hands-on experience with technologies such as Active Directory (AD), System Center Configuration Manager (SCCM), Security Technical Implementation Guides (STIGs), Multi-Factor Authentication (MFA), Mobile Device Management (MDM), and Group Policies. These tools and technologies are critical for safeguarding digital infrastructures, and I obtained extensive knowledge with their deployment, configuration, and troubleshooting. This practical experience with enterprise-level security operations has considerably improved my technical expertise and problem-solving abilities, allowing me to effectively solve real-world difficulties.

Furthermore, my leadership role on the system administration team gave me great experience managing and mentoring others, honing my communication skills, and learning how to create teamwork in high-pressure situations. Leading a team of four taught me the complexities of balancing technical and human responsibilities managing personalities, creating clear expectations, and maintaining productivity under tight constraints. These abilities are critical for my future career, since I hope to advance to higher leadership positions in cybersecurity.

My knowledge of the Governance, Risk, and Compliance (GRC) landscape was also valuable. As part of my job, I researched access control systems, regulatory frameworks, and security clearance standards, including those particular to the Department of Defense (DoD). Gaining experience with Secret and Top-Secret clearance levels increased my understanding of the need of complying to tight security standards and regulations designed to secure sensitive data. I also worked to streamline user access management processes, automate activities, and ensure internal and external regulatory compliance. These efforts have given me a comprehensive grasp of how governance and compliance frameworks are critical to sustaining strong cybersecurity defenses.

This internship not only improved my technical skills, but it also helped me better comprehend the larger business ramifications of cybersecurity. With the rising frequency and sophistication of cyber threats, it is evident that cybersecurity is no longer just a technical issue, but rather a strategic business function that necessitates cross-departmental coordination and a thorough grasp of governance.

Looking ahead, I am enthusiastic to build on these experiences as I pursue my academic and professional goals. I am happy to announce that I have been admitted to Temple University's Master's degree in IT Auditing and Cybersecurity. This job will allow me to hone my skills and enhance my understanding of advanced cybersecurity topics, risk management, and compliance. Furthermore, the program will help me pursue certifications such as Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM), which would confirm my knowledge and prepare me for leadership roles in the sector.

This internship has been a watershed moment in my career, and I am appreciative for the practical experience and insights it has brought. The skills and information I've acquired

throughout this time will surely serve as the foundation for my future undertakings. I am excited to put what I've learned into practice and continue to improve cybersecurity processes and assist organizations in protecting their digital assets. With the combination of my academic background, hands-on experience, and future certifications, I am confident that I will be well-equipped to tackle the ever-evolving challenges of the cybersecurity landscape and contribute meaningfully to the field.

On a personal level, this internship has helped me grow as a professional and individual. It has put my adaptability and ability to learn new abilities to the test. As I handled various technical duties and leadership responsibilities, I learned to balance my strengths and areas for progress, resulting in increased self-awareness. The challenges I experienced, whether it was debugging complicated security concerns or managing a team, encouraged me to step outside of my comfort zone and develop resilience. These experiences have given me confidence in my capacity to thrive in high-stakes situations, as well as a more defined sense of purpose for my career.

Additionally, the internship taught me the value of teamwork and mentorship. As I mentored my team, I learned new leadership lessons, such as the importance of actively listening, providing constructive feedback, and supporting others' personal and professional development. The ties I've formed with colleagues and mentors over this time have been important, and I'm eager to continue cultivating these connections as I progress in my career. This experience has not only improved my technical skills, but also my interpersonal skills, which I believe will be useful as I advance in my career in cybersecurity.

As I near the finish of my Bachelor's degree in Cybersecurity, I reflect on the progress I've made over the years. The academic journey, combined with the hands-on experience gained

during my internship, has provided a solid foundation for the next stage of my career. It's been a challenging but rewarding path, and I'm ready to transition from the classroom to the workplace, where I can apply my knowledge to real-world cybersecurity issues. This milestone is more than just the completion of an academic degree; it is a personal achievement that shows years of dedication, perseverance, and growth. It has instilled in me a strong appreciation of the importance of continuous learning and being current in a rapidly changing industry.

Reflecting on my journey, I can trace much of my dedication to the lessons learned during my time in the US Navy. My service taught me the value of cybersecurity for both national security and operational integrity. The Navy's mission-driven environment helped me understand the critical nature of maintaining secure communications and systems, even under the pressure of high-stakes situations. The discipline and adaptability I developed during my military service have been key to my success in transitioning to cybersecurity, where these skills are just as vital in securing complex infrastructures and responding to evolving threats. This foundation has provided me with a unique perspective on the convergence of physical and digital security, preparing me to face the multifaceted challenges of modern cybersecurity.

In many respects, the Navy influenced my approach to problem solving and risk management skills that are critical in the cybersecurity sector. I learnt how to remain calm under pressure, think critically, and solve problems with accuracy and forethought. The shift from military service to academic life was difficult, but the resilience and perseverance I developed throughout my time in the Navy enabled me to adjust swiftly to the rigorous demands of my degree.

With a bachelor's degree in cybersecurity, I am happy of how far I have come, from a structured atmosphere in the Navy to the academic world, and now into a professional position in

cybersecurity. My military experience has reinforced the importance of a secure, resilient infrastructure, and as I prepare to enter the cybersecurity industry, I am confident that I will use both my technical skills and leadership abilities in the same way that I did while serving ensuring safety, security, and operational excellence.

4- References:

Aljuboor, M. (2024, November 12). Personal communication.

5- Appendices:

Sample #1:

```
#!/bin/bash

# For loop to print numbers from 0 to 10
echo "Printing numbers from 0 to 10 by for loop: "
for ((i = 0; i <= 10; i++)); do
    echo $i
done

echo

# Using while loop to print numbers from 0 to 10
echo "Printing numbers from 0 to 10 using while loop: "
count=0
while [ $count -le 10 ]; do
    echo $count
    ((count++))
Done
```

This Bash script shows how to use a for loop and a while loop to output values ranging from 0 to 10. The for loop is used when you know exactly how many iterations

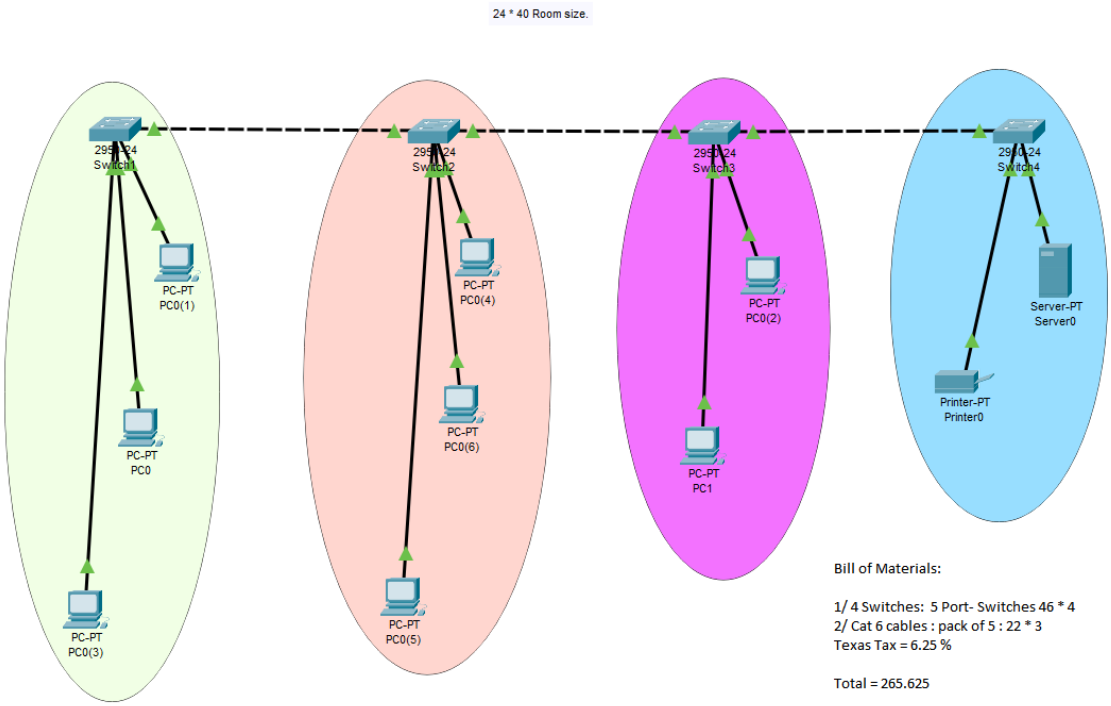
are required. In this scenario, it begins at 0 and proceeds until it reaches 10, printing each number as it goes. The while loop, on the other hand, runs indefinitely if a condition is met. In this script, the loop begins with a count of 0 and continues until the count exceeds 10, outputting each number and incrementing the count by one in each iteration. Both loops achieve the same objective, although they use different iteration methods.

Sample #2:

```
#!/bin/bash for i in {1..254};do (ping -c 1 192.168.10.$i > /dev/null && echo 192.168.10.$i &); done
```

This script is useful for network administrators or security professionals who need to quickly discover live devices on a local network. It helps in identifying active IP addresses in a subnet, which is a fundamental step in network monitoring, troubleshooting, or penetration testing. By using the ping command, the script efficiently checks for online devices without sending excessive traffic. The parallel execution (with &) ensures that the process runs faster by executing multiple pings at once, which is ideal for larger networks or quicker assessments.

Sample #3:



This diagram depicts the design and cost analysis of a small network configuration for a 24 x 40 room. The network is made up of four switches (2950-24), each of which connects to several devices, including nine PCs, a server, and a printer. These devices are divided into four separate subnets for logical segmentation. A backbone link connects the switches, allowing for communication throughout the network. The green, red, pink, and blue zones correspond to different areas of the network, with each subnet assigned specific devices. The arrangement uses Cat 6 cables for communication, and the entire cost, including hardware and a Texas tax rate of

6.25%, is $265.625. This network models an educational or small business environment, with a focus on device interconnection, network segmentation, and cost-effectiveness.