# BSIS Program Review Part 2: Key Assignments and Career Preparation

## Introduction

As I reach the final stage of my Bachelor of Science in Information Science (BSIS) program, I have been privileged to undertake diverse assignment sets that enabled me to acquire skills that are relevant for a career in the information security and technology field. Among all the assignments during my upper-level courses, some of them were highly impactful in preparing me for the actual professional tasks that I hope to perform. This essay identifies two tasks that I think were most critical and worthwhile during my studies in the BSIS program: the Ethical Hacking lab project in CIS 4202 and the Security Risk Assessment Report in CIS 4361.

## Ethical Hacking Lab Project – CIS 4202: Ethical Hacking

- In the Ethical Hacking course, a prominent assignment was the hands-on lab project that saw us simulate network threats and conduct defensive cybersecurity measures to counter threats. The project started with scanning and mapping network systems with tools such as Nmap and Wireshark and progressed to identifying vulnerabilities, suggesting security measures, and making reports on our findings. This project succeeded in filling the gap in my understanding of real-world cybersecurity tools and techniques. This exercise was most useful in that it was applicable to real work—to the kind of work cyber security professionals do on a daily basis. By applying theory into practice, I established my expertise in using technical tools and techniques to combat cyberattacks and solidified my interest in penetration testing and threat analysis as a profession.

## Security Risk Assessment Report – CIS 4361: Management of Health Information Systems Security

- As part of the Management of Health Information Systems Security course, we had to design an end-to-end Security Risk Assessment Report for a sample healthcare organization. This exercise asked us to assess likely vulnerabilities in physical, network, and data environments, and suggest remediation with best information security practices. In addition to the above, we had to take into account HIPAA guidelines and any other regulatory compliance requirements of the healthcare industry. This exercise was highly impactful because it brought together both technical and administrative sides of cybersecurity. It provided me with a better overall understanding of security planning and risk management, skills that can be applied to nearly any information security position. Report

writing demanded careful thought, careful detail attention, and good communications—skills that will be valuable as I transition into policy creation or IT compliance positions..

**Conclusion**

- The Security Risk Assessment Report and the Ethical Hacking lab project stood out as the best in my BSIS course work. They both enabled me to become very close to the subject matter, apply what I know to real-life situations, and be confident about my technical and analytical skills. These assignments not only enhanced my cybersecurity skills but also equipped me to handle the duties and challenges that I will face in a workplace. In my professional career, I will take with me the learning and experiences from these assignments as a starting point for ongoing improvement and success in the information security industry.