What we did:

Our audit team assessed the Internet connection, computer systems, and data processes in Dr. King's Office at West Texas A&M University. The audit plan was used to guide the audit procedure, and our team worked closely with Dr. King and the staff to document their observations.

What are the results:

During the audit, our team found that the Internet connection in Dr. King's Office was stable and reliable, meeting the needs of the office. The computer systems were up-to-date, secure, and functional, and the data processes were efficient, accurate, and secure. However, the audit team also found the following top five findings:

Item #1: Some staff members were using weak passwords, which could make it easier for hackers to gain access to the office's computer systems.

Item #2: Some computers had outdated antivirus software, which could put the entire network at risk.

Item #3: The office did not have a formal backup and disaster recovery plan, which could result in data loss in the event of a system failure or cyberattack.

Item #4: Some staff members did not receive regular cybersecurity awareness training, which could leave them vulnerable to phishing scams and other types of cyberattacks.

Item #5: The office did not have a formal process for monitoring and detecting security incidents, which could delay the response time to a cyberattack.

What your recommendations:

To address the above findings, we recommend the following:

Item #1: The office should enforce a strong password policy and require staff members to use strong passwords that are difficult to guess. This can be implemented easily and quickly, with the support of training programs.

Item #2: The office should upgrade all antivirus software to the latest version and ensure that the software is updated regularly. This should be done in the short term and integrated into the office's maintenance policy.

Item #3: The office should develop a backup and disaster recovery plan that includes regular data backups and testing of the recovery process. This plan should be reviewed and updated regularly.

Item #4: The office should provide regular cybersecurity awareness training to all staff members to ensure they are up to date on the latest threats and how to protect themselves and the office. The training should be included as part of the onboarding process and ongoing annual training.

Item #5: The office should establish a formal process for monitoring and detecting security incidents, such as the use of security information and event management (SIEM) software. This can be done in the short term by implementing an automated system that alerts the IT team in case of a security incident.

What is their risk posture:

Based on our assessment, Dr. King's Office has a low-risk posture, given the stable and reliable Internet connection, secure computer systems, and efficient data processes. However, the weak passwords, outdated antivirus software, lack of backup and disaster recovery plan, insufficient cybersecurity awareness training, and absence of a formal incident response plan, pose the greatest risks to the office. To mitigate these risks, we recommend implementing the above recommendations and conducting regular security audits to ensure that the office's security posture remains strong.