Use the Case study of AfriTech Innovations to answer any two questions below.

Question 1 (10 marks): Describe the different types of security testing methodologies employed by AfriTech Innovations in ensuring the integrity and security of the electronic election voter system. Discuss the significance of Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) in identifying vulnerabilities. Explain how these testing methods contributed to the overall security of the system.

Question 2 (10 marks): Analyze the challenges faced by AfriTech Innovations during the development process, specifically focusing on the oversight related to data transmission encryption. Discuss the impact of this oversight on the system's security and the measures taken by AfriTech to rectify the issue. Evaluate the effectiveness of their response and the strategies employed to enhance the encryption protocol.

Question 3 (10 marks): Investigate the role of Penetration Testing in AfriTech Innovations' security testing approach. Explain how ethical hacking was utilized to simulate cyberattacks on the electronic election voter system. Discuss the findings and the actions taken based on the penetration testing results. Evaluate the importance of such testing methodologies in identifying vulnerabilities and ensuring the system's resilience against real-world threats.

Question 4 (10 marks): Explore the overall impact of AfriTech Innovations' secure application testing practices on the national elections in Kenya. Discuss how their rigorous testing approach influenced the transparency, accuracy, and accessibility of the electoral process. Analyze the long-term implications of their security measures on the public's trust in electronic voting systems and the lessons that can be extrapolated for future projects in similar contexts