Republic of the Philippines
Laguna State Polytechnic University
Province of Laguna

Name: _____JACOB B. CORTES_____

Section: _____BSIT WMAD_____

Performance Task 2 – Part 1

Answer the following set of questions:

1. What is the significance of system architecture in the context of information assurance and security?
    - System architecture is the backbone of information assurance and security. It's like the blueprint that shapes how a system is built to be secure from the start. Designing security measures into the system early on, it helps prevent problems before they even happen. It also helps protect important data and resources, making sure they stay safe and available when needed.
2. How does the choice of system architecture impact the overall assurance and security of information?
    - The choice of system architecture profoundly impacts how secure and resilient a system is. An architecture designed with security in mind reduces vulnerabilities, improves risk management, and ensures that the system can withstand evolving threats.
3. How can a well-designed system architecture improve the integration of security components?
    - A well-designed system architecture serves as the foundation for seamlessly integrating security components. It allows security features to be embedded from the start, ensures efficient communication

between security layers, and provides scalability and flexibility for future growth.

4. How can a system architecture be designed to accommodate growth and changes in assurance of information and security requirements?

    - A system architecture designed for growth and adaptability ensures that security measures evolve alongside the organization's expanding needs. Focusing on scalability, modularity, automation, and flexibility, the architecture can accommodate new security requirements, technologies, and compliance standards.

5. If you put yourself as a developer/programmer, what do you think are the key components to be involved in ensuring the security of information within a system?

    - As a developer, ensuring the security of information within a system requires a comprehensive and proactive approach. By integrating security into the development process from the start and following best practices for coding, testing, and deployment, you can minimize the risk of security breaches and protect sensitive data.

6. How do hardware and software components collaborate to create a secure information environment?

    - Software components is fundamental to building a secure information environment. Hardware provides the physical security features that ensure sensitive data is protected against unauthorized access, tampering, or theft, while software adds flexibility and intelligence to manage security policies, authentication, encryption, and monitoring.

7. What role do you think assurance plays in building confidence in the security of information systems?

    - It provides evidence that the security measures in place are effective, reliable, and in compliance with established standards and regulations.

8. Provide and discuss one security models commonly employed in information security.

    - The Bell-LaPadula model is an essential framework for ensuring confidentiality in highly controlled environments, especially where the protection of sensitive information is critical. By enforcing clear access

controls based on classification levels and restricting both read and write actions, it ensures that information is only accessed and modified by authorized personnel.

9. Provide and discuss common challenges faced in assuring the security of information within complex systems.

    - Ensuring the security of information in complex systems requires addressing a wide range of challenges that arise from the system's size, diversity, evolving threats, and dynamic nature. It demands a multi-layered approach, combining strong access controls, continuous monitoring, risk management, robust incident response, and effective integration of security practices across the entire system.

10. How can organizations ensure both assurance and compliance in their information security practices?

    - Ensuring both **assurance** and **compliance** in information security practices is essential for organizations to protect sensitive information, manage risks, and meet regulatory and industry standards. Assurance provides confidence that security measures are effective, while compliance ensures that the organization meets legal, regulatory, and industry-specific requirements.