Republic of the Philippines
Laguna State Polytechnic University
Province of Laguna

ISO 9001:2015 Certified
Level I Institutionally Accredited

Name: Jervin B Guevarra
Section: BSIT IV- 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 crucial for information assurance and security as it defines how information is processed, helps identify vulnerabilities, supports layered defenses, and enables the integration of security measures to mitigate risks

2. How does the choice of system architecture impact the overall assurance and security of information?

   The choice of system architecture directly impacts information assurance and security by determining the system's ability to prevent, detect, and respond to threats.

3. How can a well-designed system architecture improve the integration of security components?

   A well-designed system architecture improves the integration of security components by ensuring they work cohesively within the system. It provides a clear framework for incorporating encryption, authentication, firewalls, and monitoring tools in a way that enhances their effectiveness.

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

   A system architecture can be designed to accommodate growth by being modular and scalable. Modular design means that components can be added or updated without overhauling the entire system. Scalability allows for expanding security features as the system grows. It's also important to use flexible frameworks and regularly review

security needs to adjust to evolving threats.

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?

   Encryption: To protect data in transit and at rest.
   Authentication and Authorization: Ensuring only the right users have access.
   Firewalls and Intrusion Detection Systems (IDS): To monitor and block unauthorized access.
   Audit Logs: Keeping records of all access to detect suspicious activities.
   Regular Updates: Keeping software up to date to patch vulnerabilities.

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

   Hardware components like firewalls, servers, and network devices provide physical barriers and control the flow of information. Software components like antivirus, encryption tools, and access controls add an additional layer by securing data and user activities.

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

   Assurance builds confidence by proving that a system is reliable and secure. It includes regular audits, testing, and certifications to show that security measures are effective and meet standards.

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

   The Bell-LaPadula Model is a common security model, focused on confidentiality. It uses the principle of "no read up, no write down", meaning users cannot access data above their security level, and they cannot write to a lower security level, preventing leakage of sensitive information.

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

   Some common challenges include:

- **Complexity: Large systems have many components, making it hard to secure every part.**
- **Evolving Threats: Attack methods change, so security must constantly adapt.**
- **Human Error: Mistakes like misconfigurations or poor password practices can create vulnerabilities.**
- **Legacy Systems: Older systems may not support modern security practices, making integration tough.**

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

Organizations can ensure assurance and compliance by:

- **Following security standards like ISO/IEC 27001 or NIST.**
- **Conducting regular audits and vulnerability assessments.**
- **Training employees on security best practices.**
- **Implementing clear policies that meet regulatory requirements, ensuring security and compliance are embedded in daily operations.**