Adventist University of Central Africa
P.O. Box 2461 Kigali, Rwanda | www.auca.ac.rw | info@auca.ac.rw

Faculty of Information Technology

MID-SEMESTER EXAMINATION

Course: INSY 421 / Software Security **Academic Year: 2022-2023**

Instructor: Mr. Ernest Condo **Date:**

INSTRUCTIONS:

- Timing: 2h:00
- Follow the order of questions
- Choose all questions from Section A & B

SECTION A: /10 Pts

1. Physical controls help safeguard physical devices, equipment, and facilities that house sensitive data or provide access to critical systems. Some examples physical control are:
   - **A. Access controls**
   - **B. Intrusion detection systems (IDS)**
   - **C. None of the above**
2. Hacktivists Refer to the hackers who are driven by a cause like social change, political agendas, or terrorism.
   A. True **B. False**
3. Technical controls are security measures that are implemented within software to protect against unauthorized access, manipulation, or disclosure of sensitive data. Some common examples of technical controls in software security include:
   - **A. Security guards**
   - **B. Locks and keys**
   - **C. None of the above**
4. Advanced Persistent Threats refer to highly trained and funded groups of hackers with covert and open-source intelligence at their disposal.
   A. True **B. False**

5. Administrative controls are an important aspect of software security and involve establishing policies, procedures, and guidelines to manage and protect software systems. Some common administrative controls in software security include:

   A. Access control

   B. Security policies and procedures

   C. All the above are correct

6. Defect are problems at a deeper level. They are instantiated in the code and present or absent at design-level.

   A. False **B. True**

7. Useful source code analysis tools must:

   A. Be extensible.

   B. Be designed for security.

   C. All the above are correct

8. Critical Aspects of Architectural Risk Analysis:

   A. Weakness Analysis

   B. Ambiguity Analysis

   C. All the above are correct

9. Adversarial security testing - Refer to Testing mechanisms that ensure that functionality is well implemented.

   A. False **B. True**

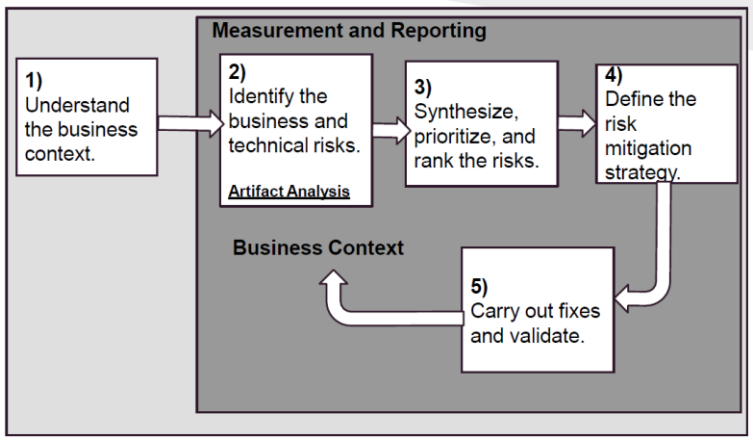
10. Functional security testing - Refer to Risk-based security testing motivated by understanding the attacker's approach.

    A. False **B. True**

SECTION B / 20MARKS

1. Security Requirements cover both functional security and emergent characteristics. State and explain three criteria satisfying security requirement. **/6 Marks**
   - Cover both functional security and emergent characteristics.
   - Satisfy three criteria:
     - **Definition:** Must be explicitly defined what security requirements are.
     - **Assumption:** Must take into account the assumptions that the system will behave as expected.
     - **Satisfaction:** Security requirements must satisfy the security goals, and the system must satisfy the security requirements.

2. Using a diagram explain the Risk management framework (RMF) stages. **/6 Marks**



3. What is SQL Injection and give three main types. **/4Marks**

   Types of SQL Injections

   SQL injections typically fall under three categories: In-band SQLi (Classic), Inferential SQLi (Blind) and Out-of-band SQLi. You can classify SQL injections types based on the methods they use to access backend data and their damage potential.

4. Write in full and differentiate the CSRF vs IDOR**. /4Marks**

What is the full form of IDOR?

Insecure direct object references (IDOR) are a type of access control vulnerability that arises when an application uses user-supplied input to access objects directly.

What is CSRF with example?

Cross site request forgery (CSRF) is a vulnerability where an attacker performs actions while impersonating another user. For example, transferring funds to an attacker's account, changing a victim's email address, or they could even just redirect a pizza to an attacker's address!

Good Luck!