IAS INFORMATION ASSURANCE and SECURITY

Learning Evaluation

Name: Mary Rose M. dela Torre **Section: BSIT 3C (T209)**

Activity B

Instruction:

Based from the lesson read about the introduction of information security, provide what is asked on the statements below. Write your answer on the space provided.

Guide questions:

1. **A successful organization should have the multiple layers of security in place for the protection of its operations. What are this layers and the security features it covered**?

   To ensure the safety of each organization you should know how to tighten the security in other to protect the confidentiality of the information. The followings are the multiple layer of security:

   - **Physical security-** is the protection of people, property, and physical assets from actions and events that could cause damage or loss. Though often overlooked in favor of cyber security, physical security is equally important**.**
   - **Personal security-** is the main focus of this guide and specifically relates to entities taking reasonable steps to protect personal information including sensitive information from misuse, interference and loss, as well as unauthorized access, modification or disclosure
   - **Operations security**- is an analytical process that classifies information assets and determines the controls required to protect these assets. Originated as a military term that described strategies to prevent potential adversaries from discovering critical operations-related data. As information management and protection has become important to success in the private sector.
   - **Communications security**- the protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study.

- **Network security-** consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator.
- **Information security –** is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be physical or electronic one. Information can be anything like your details or we can say your profile on social media, your data in mobile phone, your biometrics etc. Thus Information Security spans so many research areas like Cryptography, Mobile Computing, Cyber Forensics, and Online Socia Media.
-

2. Describe the C.I.A. triangle.

The CIA Triangle is a security model that highlights core data security objectives and serves as a guide for organizations to keep their sensitive data protected from unauthorized access and data exfiltration. C.I.A was standard based on confidentiality, integrity, and availability. Confidentiality it helps to ensure that sensitive data is only accessible by authorized individuals, the first step is to eliminate global access to sensitive data. Integrity is an essential component of the CIA Triad and designed to protect data from deletion or modification from any unauthorized party, and it ensures that when an authorized person makes a change that should not have been made the damage can be reversed. . Availability helps to run smoothly when data is readily available and accessible. However, when a security incident occurs preventing access or yielding too much access a strong audit capability can assist and determine the root cause. CIA Triad is all about information it promotes a limited view of the security that ignores other important factors.

3. What are the six components of an information system?

The six components of information system are:

- **Hardware-** It is a physical components which is used to store the data present in the system like input and output devices.
- **Software –** is a collection of programming languages used for execution.
- **People-** the user or the system operators who have the knowledge of accessing the data presented in the system.

- **Database-** the collection of structured or organized data which is used in different processes.
- **Procedures-** the policies which are used to govern the process in a secure manner to complete the task assigned.
- **Networking-** the link used to connect more than one system to exchanged data.

a) What is a procedure in IS and why is it important in information systems?

Any business can be successful only when there is a consistent management of organizational and financial data with efficient information systems. Most of the companies have seen a drift in the process of workflow due to the accuracy and reliability. There is no alternative for the right information at the required time in the world of business where every industry revolves round the Internet of Things. This raised the need to innovate and develop the systems that can be implemented to make information accurate that can be quickly accessed on demand. An effective information system can entitle an organization with better planning, decision-making and hence desired results.

4. On the Approaches to Information Security Implementation, what is the difference between the Top-Down-Approach and the Bottom-Up-Approach?

Top-Down Approach utilize the top-down approach in order to assess, determine, and implement business decisions made by upper executives. The processes are streamlined and communicated to lower rank employees, who carry out these tasks. Consequentially, projects are more easily managed, and risk is decreased significantly due to strategic decisions created from the top management. This approach relies on the executive level to decide how to prioritize, manage, and conduct everyday processes.

Bottom-up communication revolves around the inclusion of all employees, their ideas, and their perceptions of the business in order to make the most informed decisions. In this case, a business invites the entire team to participate in the company's management and decision-making process. This process allows the company to identify its most targeted and most appropriate goals.

The top-down approach can spawn many positive business impacts through unique aspects of management, including creating clear lines of authority, standardizing products and services, facilitating quality control and streamlining tasks and achieving goals quickly. By comparison, the bottom-up approach utilizes alternative ways of management to achieve success. These can include forming a unique perception of the company, its goals, and its employees, measuring operational risk, reallocating assets and decision-making power and giving voice to all employees.

5. **On the six phases of the Systems Development Life Cycle, explain one phase and elaborate the process in securing that particular phase.**

Software Development Life Cycle is a process used to develop software. There are different stages or phases within the software development life cycle and in each phase, different activities take place. The 5th phase of Software Development Life Cycle is the implementation phase.

Implementation

After the requirements and design activity is completed, the next phase of the SDLC is the implementation or development of the software. In this phase, developers start coding according to the requirements and the design discussed in previous phases. Database admins create the necessary data in the database, front-end developers create the necessary interfaces and GUI to interact with the back-end all based on guidelines and procedures defined by the company.

During implementation, the project team creates the actual product. Product implementation can be an exciting phase for the customer, because their idea for the project becomes something tangible. Project developers begin building and coding the software. Developers also write unit tests for each component to test the new code that they have written, review each other's code, create builds and deploy software to an environment. This cycle of development is repeated until the requirements are met.

For example, if a customer wants a new gaming application, the project developers must program the application to perform the customer's gaming requirements. As the team develops the code, the team must follow specific coding requirements. Customer requirements may call for specific computer programming languages or upgrades, and developers need to run the applications to ensure they function properly.