IAS INFORMATION ASSURANCE and SECURITY

LEARNING EVALUATION

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

Activity C

Instruction:

Based from the last lesson read, provide what is asked on the statements below. Write your answer on the space provided.

Guide questions:

1. **How the Chief Information Officer (CIO) differ from the Chief Information Security Officer (CISO)?**

Chief Information Officer (CIO) and Chief Information Security Officer (CISO) both work with each other within the organization. Each of them plays important role to insure the safety of an organization.

Chief Information Officer (CIO) are tasked to ensure the company's business process are running efficiently. They are the one who thinks how to implement the new technologies in order to modernize the services they provide. CIO typically works on the business management parts of the organization and is more internally and operationally focused with their tasks. The CIO might have to check for proper alignment of security processes at various stages of business.

On the other hand, Chief Information Security Officer (CISO) is positioned to protect data and assets from potential information security risks in an organization. CISO or will typically report to the CEO. The CISO was brought into the modern organization to monitor and analyze potential security risks for the organization.

As a whole, Information Security becomes more prominent in the corporate world, the collaborative roles of CIO & CISO are of utmost importance. Both go hand in hand and requires a mutual agreement in various risk critical decisions to ensure better business continuity and development. The CISO will take a management role to implement these responsibilities. For a smaller enterprise, the CIO may be involved in execution of some or all of these measures or provide oversight for vendors.

2. **Differentiate "Information security management and professionals" to "Information technology management and professionals".**

Information security management and professional are the responsible for developing and managing Information System Cyber Security, including disaster recovery, database protection and software development. Manages IS security analysts to ensure that all the application are functional and secure. It develops and deliver IS security standard, best practice and system to ensure information system security across the enterprises. It is a set of policies and procedures for systematically managing an organization's sensitive data. The goal of an ISMS is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security breach.

Information technology management includes many of the basic functions of management, such as staffing, organizing, budgeting and control, but it also has functions that are unique to IT, such as software development, change management, network planning and tech support. It may composed of Software Applications Developer, Information Security Analyst, Computer Systems Analyst, Database Administrator, Management Analyst, and Computer Network Architect.