Name: Rogel R. Gerodiaz Teacher: Malig-On, Rodolfo  
Grade&Section: BSIT-32E1  
  
  
  
**1.** **What is Information Assurance & Security (IAS)?** Information Assurance and Security (IAS) is a field that manages and protects information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This involves providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

**2. Why do we need to study IAS?** The study of IAS is crucial in today's digital age where data breaches, identity theft, and cyber-attacks are common. By studying IAS, individuals learn how to protect sensitive information and systems from cyber threats. This knowledge is essential in many fields, including business, healthcare, finance, and government. Understanding IAS can lead to better personal data management and opens a variety of career opportunities in the growing field of cybersecurity.

**3. Difference between Information Assurance and Information** Security Information Security is a component of Information Assurance. While Information Security is focused on protecting data from being compromised (through encryption, secure networks, etc.), Information Assurance is a broader field that not only includes security measures but also focuses on ensuring the reliability and accuracy of data. Information Assurance involves a strategic risk management approach, ensuring that data is reliable and can be trusted, and that systems are resilient to potential attacks or disruptions.

**4. The Five Pillars of IAS**

* **Confidentiality:** This involves ensuring that data is not made available or disclosed to unauthorized individuals, entities, or processes. Techniques like encryption and secure channels are used to protect the confidentiality of data.
* **Integrity:** This ensures that data is accurate and complete and has not been tampered with or altered by unauthorized individuals. Checksums, hashes, and digital signatures are common methods used to maintain data integrity.
* **Availability:** This ensures that data and resources are available to authorized users when they need them. This involves managing hardware failures, system upgrades, and ensuring systems can handle the required workload.
* **Non-repudiation:** This ensures that a party involved in communication cannot deny the authenticity of their signature on a document or the sending of a message. Digital signatures are commonly used for non-repudiation.
* **Authentication:** This involves verifying the identity of a user, process, or device. It often involves usernames and passwords but can also involve more complex methods like two-factor authentication or biometric data.