NAME: TANKISO MASOEBE

IT LAW WK 1

1. **IT Law Scenario Analysis**

An IT law scenario involves a company that collects customer data through an online platform. The company stores personal information such as names, email addresses, and payment details. Under IT laws like data protection and privacy regulations, the company is legally required to secure this data and use it only for authorized purposes. If a cyberattack occurs due to weak security measures, resulting in data leakage, the company may face legal consequences. Customers can take legal action for breach of privacy, while regulators may impose fines or penalties. IT law also requires the company to notify affected users and authorities about the breach. This scenario shows how IT law protects individuals' digital rights, enforces accountability on organizations, and promotes responsible handling of information systems. Compliance with IT law helps reduce legal risks, maintain trust, and ensure ethical use of technology.

2. **Legal Framework Research**:

A legal framework is the system of laws, regulations, and guidelines that govern activities within a country or organization. It establishes rules for behavior, protects individual rights, and ensures justice and fairness. Legal frameworks cover areas such as criminal law, civil law, labor law, and information technology law. Governments create and enforce these laws through institutions like courts and regulatory bodies. A strong legal framework promotes stability, accountability, and social order by clearly defining responsibilities and penalties. In modern societies, legal frameworks also adapt to new challenges such as cybercrime, data protection, and digital transactions.

3. **Case Study Review**:

This case study examines a data breach incident in a financial organization where hackers gained unauthorized access to customer records. The breach occurred due to weak password policies and outdated security systems. As a result, sensitive information such as account numbers and personal details were exposed. The organization faced legal action under data protection laws and suffered reputational damage. The case highlights the importance of complying with IT laws, implementing strong cybersecurity measures, and training employees on data protection practices. It demonstrates how failure to follow legal and technical standards can lead to serious legal and financial consequences.

4. **Compliance Checklist with Explanation**:

A compliance checklist helps organizations ensure they follow legal and regulatory requirements. Key items include data protection policies, secure password management,

regular system updates, user access control, and employee training. Organizations must also conduct routine audits, maintain proper documentation, and report security incidents promptly. Following this checklist reduces the risk of legal penalties, data breaches, and operational failures. Compliance ensures that information systems operate legally, securely, and ethically. By regularly reviewing and updating the checklist, organizations can adapt to new laws and emerging technology risks, maintaining trust with users and regulatory authorities.