NAME: TANKISO MASOEBE

IT LAW WEEK 3

1.SCENARIO ANALYSYS:

In a hospital system, applying the NIST Cybersecurity Framework (CSF) and GDPR regulations helps reduce risks from ransomware attacks while ensuring ethical management of patient data. NIST CSF guides hospitals through Identify, Protect, Detect, Respond, and Recover stages. By implementing strict access controls, network segmentation, regular data backups, and continuous monitoring, hospitals reduce the likelihood of CXransomware infections and minimize operational disruption. GDPR complements this by enforcing strict rules on personal data storage, processing, and breach notifications, ensuring patient privacy is respected. Staff training on cybersecurity best practices and GDPR awareness increases preparedness and reduces human error, a common vulnerability. Together, these frameworks lower financial, legal, and reputational risks. They also foster ethical responsibility, maintaining patient trust by demonstrating a commitment to confidentiality and compliance. Integrating NIST CSF and GDPR ensures hospitals are not only technically secure but also aligned with legal and moral obligations.

2.CONCEPT RESEARCH:

Enforcement agencies regulate IT compliance by ensuring organizations follow legal and ethical standards. The Federal Trade Commission (FTC) in the U.S. enforces consumer protection and data privacy, penalizing companies for unsafe practices, such as weak cybersecurity or misleading data collection. The Information Commissioner's Office (ICO) in the U.K. oversees GDPR compliance, issuing fines for breaches and guiding organizations on personal data handling. These agencies encourage companies to implement strong security measures, maintain transparent policies, and conduct regular audits. For example, a hospital failing to secure patient records could face ICO fines, while an e-commerce site misusing customer data may be sanctioned by the FTC. Their oversight promotes accountability and reduces risks associated with data breaches.

3.TOOL PRACTICE:

Using Adobe Acrobat to annotate a PDF of the Budapest Convention enhances comprehension and retention. Highlighting key provisions, such as

definitions of cybercrime, jurisdiction rules, and international cooperation measures, helps identify the most critical points quickly. Adding comments and notes allows connections between clauses, highlighting implications for cybersecurity compliance and policy enforcement. This process encourages active reading, enabling deeper understanding of legal responsibilities and reporting obligations. Annotating also makes it easier to reference important sections in discussions or assignments. Overall, using Acrobat transforms a static legal document into an interactive learning tool, improving clarity, organization, and practical application of the Budapest Convention's provisions.

4.APPLICATION PRACTICE:

In a fictional company offering payment apps, a PCI-DSS compliance policy ensures secure handling of cardholder data. The policy defines encryption standards for data in transit and at rest, enforces strong access controls, and mandates regular vulnerability scans and penetration testing. Employee training emphasizes secure coding and incident reporting. Integration into the app development lifecycle ensures that security measures are applied from design to deployment, reducing the risk of data breaches and fraud. By embedding PCI-DSS requirements into daily operations, the company protects customer information, maintains regulatory compliance, and builds trust. This approach balances technical security, operational consistency, and legal accountability across all payment services.