Kompliance Krew
In-Class Exercise - 11
CSF table for Ransomware

CSF Function	Category	Subcategory	Application to Ransomware
Govern (GV)	Risk Management Strategy (GV.RM)	GV.RM 01: The organizational mission is understood and informs cybersecurity risk management	A good risk management strategy ensures that the organization's stakeholders understand the approach to identifying, assessing, and mitigating ransomware risks. The factors in place foster a unified response to potential threats.
Identify (ID)	Asset Management (ID.AM)	ID.AM 01: Inventories of hardware managed by the organization are maintained	Maintaining and finding the devices that are vulnerable assets that could be targeted by ransomware enables proactive protection measures.
Protect (PR)	Data Security (PR.DS)	PR.DS 01: The confidentiality, integrity, and availability of data-at-rest are protected	Securing the data at rest using encryption like AES 256 and having proper access control will reduce the chance of unauthorized access and breaches, mitigating the impact of ransomware attacks.
Detect (DE)	Continuous Monitoring (DE.CM)	DE.CM 01: Networks and network services are monitored to find potentially adverse events	Continuous monitoring will allow early detection of malicious or abnormal activities like ransomware, facilitating prompt response and containment.
Respond (RS)	Incident Mitigation (RS.MI)	RS.MI 01: Incidents are contained	Having measures and procedures to contain ransomware incidents can prevent the spread of malware and limit damage

			to the organization.
Recover (RE)	Incident Recover Plan Execution (RC.RP)	RC.RP 01: The recovery portion of the incident response plan is executed once initiated from the incident response process	A recovery plan ensures the organization can restore critical systems and data promptly after a ransomware attack, minimizing downtime and operational impact. All incident response personnel have detailed knowledge of ransomware recovery plans and have the authorizations needed to implement each aspect of such plans