Name: Olofin Iyiola
Cybersecurity Assignment 2

QUESTION: Using the NIST CSF 2.0, explain in a tabular form how to identify, protect, detect, respond, recover and govern the potential risk faced with the asset of technology and software development industry.

Sensitive Company Data in the Technology and Software Development Industry **faced insider threat attack**, the NIST CSFmanagement implementation strategy is discussed to manage this threat.

ASSET: Sensitive Company Data

Risk Category	**Identify**	**Detect**	**Protect**	**Respond**	**Recover**	**Govern**
Insider Threat	- Use cyber threat intelligence to maintain awareness of the types of threat actors likely to target the organization and the TTPs they are likely to use. - Perform threat hunting to	- Review logical and physical access privileges periodically and whenever someone changes roles or leaves the organization, and promptly rescind privileges that are no longer needed. - Take attributes of the requester and the requested resource into account for authorization decisions (e.g., geolocation,	- Use behavior analytics software to detect anomalous user activity to mitigate insider threats. - Monitor logs from logical access control systems to find unusual	- Securely share information consistent with response plans and information sharing agreements. - Voluntarily share information about an attacker’s	- Begin recovery procedures during or after incident response processes. - Make all individuals with recovery responsibilities aware of the plans for recovery and the	- Update policy based on periodic reviews of cybersecurity risk management results to ensure that policy and supporting processes and procedures adequately maintain risk at

	look for signs of threat actors within the environment. - Implement processes for identifying internal threat actors	day/time, requester endpoint’s cyber health). - Restrict access and privileges to the minimum necessary (e.g., zero trust architecture) - Periodically review the privileges associated with critical business functions to confirm proper separation of duties	access patterns and failed access attempts. - Continuously monitor deception technology, including user accounts, for any usage	observed TTPs, with all sensitive data removed, with an Information Sharing and Analysis Center (ISAC). - Notify HR when malicious insider activity occurs. - Regularly update senior leadership on the status of major incidents	authorizations required to implement each aspect of the plans. - Select recovery actions based on the criteria defined in the incident response plan and available resources. - Change planned recovery actions based on a reassessment of organizational needs and resources.	an acceptable level. - Provide a timeline for reviewing changes to the organization’s risk environment (e.g., changes in risk or in the organization’s mission objectives), and communicate recommended policy updates. - Update policy to reflect changes in legal and regulatory requirements. - Update policy to reflect changes in technology (e.g., adoption of artificial intelligence) and changes to the business (e.g.,

						acquisition of a new business, new contract requirements)

Use cyber threat intelligence to maintain awareness of the types of threat actors likely to target the organization and the TTPs they are likely to use

Ex2: Perform threat hunting to look for signs of threat actors within the environment

Ex3: Implement processes for identifying internal threat actors