Identify (ID)

Governance (GV):

1. **Does the business have a formalized cybersecurity policy?**
   - **ID.GV-1 (Policies, processes, and procedures are established and maintained).**
   - **Explanation:** Tier 1 organizations typically do not have formalized cybersecurity policies. If the business lacks a documented cybersecurity policy, it is likely in Tier 1.
2. **Is cybersecurity considered in the business's strategic goals and objectives?**
   - **ID.GV-2 (Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners).**
   - **Explanation:** In Tier 1, cybersecurity is often not integrated into strategic goals and decision-making processes. If cybersecurity is not part of the business's strategic considerations, this suggests a Tier 1 classification.
3. **Is there a dedicated cybersecurity team or personnel?**
   - **ID.GV-3 (Roles and responsibilities for cybersecurity are established and communicated).**
   - **Explanation:** Tier 1 organizations often lack dedicated cybersecurity personnel. If the business does not have staff specifically responsible for cybersecurity, it might belong to Tier 1.
4. **Are cybersecurity responsibilities assigned to specific individuals or teams?**
   - **ID.GV-3 (Same as above: Roles and responsibilities for cybersecurity are established and communicated).**
   - **Explanation:** In Tier 1 organizations, cybersecurity responsibilities are often not clearly defined or assigned. If the business does not have clearly defined roles for cybersecurity, it is an indicator of Tier 1.
5. **How does the business handle compliance with cybersecurity regulations and standards?**
   - **ID.GV-4 (Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed).**
   - **Explanation:** Tier 1 organizations often have minimal or no focus on compliance. If the business is not actively engaged in meeting regulatory or standard compliance, it may be a Tier 1 organization.
6. **Does the business utilize cybersecurity best practices and frameworks?**
   - **ID.GV-5 (Governance and risk management processes address cybersecurity risks).**
   - **Explanation:** In Tier 1, organizations generally do not follow established best practices or frameworks. If the business is not using recognized cybersecurity frameworks, this is indicative of Tier 1.
7. **Does the business have a documented cybersecurity budget?**

    - **ID.GV-2 (Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners, which includes budget considerations).**
    - **Explanation:** In Tier 1, there is often no dedicated budget for cybersecurity. If the business does not allocate specific resources for cybersecurity, it is likely in Tier 1.

Risk Assessment (RA): 8. **How does the business approach risk management in cybersecurity?**

- **ID.RA-3 (Threats, vulnerabilities, likelihoods, and impacts are used to determine risk).**
- **Explanation:** Tier 1 organizations usually have ad hoc or reactive risk management processes. If the business lacks a structured approach to cybersecurity risk management, it likely fits Tier 1.

9. **Does the business conduct regular cybersecurity audits or assessments?**
    - **ID.RA-2 (Cybersecurity risks are assessed using a risk assessment process).**
    - **Explanation:** Tier 1 organizations generally do not conduct regular audits or assessments. If the business does not perform periodic cybersecurity audits, it is likely a Tier 1 organization.

Risk Management Strategy (RM): 10. **Does the business regularly assess and update its cybersecurity practices?**

- **ID.RM-3 (The organization’s risk tolerance is determined and clearly expressed).**
- **Explanation:** In Tier 1, cybersecurity practices are generally not regularly updated or assessed. If the business does not have a regular review process for its cybersecurity practices, it may be classified as Tier 1.

Supply Chain Risk Management (SRM): 11. **Are third-party vendors and partners evaluated for cybersecurity risks?**

- **ID.SRM-3 (The organization understands the cybersecurity risks to its supply chain).**
- **Explanation:** Tier 1 organizations often do not assess third-party cybersecurity risks. If the business does not evaluate the cybersecurity posture of its vendors and partners, it may fit into Tier 1.

Protect (PR)

Awareness and Training (AT): 12. **What level of awareness do employees have regarding cybersecurity risks and practices?**

- **PR.AT-1 (All users are informed and trained).**
- **Explanation:** Tier 1 organizations often have low cybersecurity awareness among employees. If the business's employees are not aware of cybersecurity risks and best practices, it could be classified as Tier 1.

13. **Is there any regular cybersecurity training or awareness program for employees?**

- **PR.AT-2 (Privileged users understand their roles and responsibilities).**
- **Explanation:** Tier 1 organizations typically lack regular cybersecurity training. If the business does not provide ongoing cybersecurity training for employees, it could be considered Tier 1.

Data Security (DS): 14. **Does the business have measures in place to protect sensitive data?**

- **PR.DS-1 (Data-at-rest is protected), PR.DS-2 (Data-in-transit is protected).**
- **Explanation:** In Tier 1, there may be minimal or no data protection measures. If the business does not have effective measures to protect sensitive data, it is likely a Tier 1 organization.

Maintenance (MA): 15. **Is there a process for regularly updating and patching systems and software?**

- **PR.MA-1 (Maintenance and repair of organizational assets is performed and logged in a timely manner).**
- **Explanation:** In Tier 1, patch management processes are usually informal or non-existent. If the business does not have a regular update and patching process, it suggests a Tier 1 classification.

Detect (DE)

Security Continuous Monitoring (CM): 16. **How does the business monitor and detect potential cybersecurity threats?**

- **DE.CM-1 (The network is monitored to detect potential cybersecurity events).**
- **Explanation:** Tier 1 organizations often lack continuous monitoring and detection capabilities. If the business does not have effective threat monitoring in place, it may be categorized as Tier 1.

Respond (RS)

Response Planning (RP): 17. **Does the business have a process for identifying and responding to cybersecurity incidents?**

- **RS.RP-1 (Response plan is executed during or after an event).**
- **Explanation:** Tier 1 organizations typically lack a formalized incident response process. If the business has no structured approach to incident response, it is likely a Tier 1 organization.

Communications (CO): 18. **Are there established procedures for reporting cybersecurity incidents internally?**

- **RS.CO-1 (Personnel know their roles and order of operations when a response is needed).**
- **Explanation:** In Tier 1, there may not be established procedures for reporting incidents. If the business does not have a clear process for internal incident reporting, it likely fits into Tier 1.

Recover (RC)

Recovery Planning (RP): 19. **How does the business recover from cybersecurity incidents?**

- **RC.RP-1 (Recovery plan is executed during or after an event).**
- **Explanation:** Tier 1 organizations often lack formal recovery plans. If the business does not have a clear process for recovering from incidents, it is likely to be Tier 1.