

Govern

1. **Does the business have a formalized cybersecurity policy?**
 - **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?**
 - **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?**
 - **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?**
 - **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?**
 - **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?**
 - **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?**
 - **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.
-

Identify

8. **How does the business approach risk management in cybersecurity?**
 - **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?**

- **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.
10. **Does the business regularly assess and update its cybersecurity practices?**
- **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.
11. **Are third-party vendors and partners evaluated for cybersecurity risks?**
- **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

12. **What level of awareness do employees have regarding cybersecurity risks and practices?**
- **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?**
- **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.
14. **Does the business have measures in place to protect sensitive data?**
- **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.
15. **Is there a process for regularly updating and patching systems and software?**
- **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

16. **How does the business monitor and detect potential cybersecurity threats?**
- **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

17. Does the business have a process for identifying and responding to cybersecurity incidents?

- **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.

18. Are there established procedures for reporting cybersecurity incidents internally?

- **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

19. How does the business recover from cybersecurity incidents?

- **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.