You are a cybersecurity advisor helping small and medium-sized enterprises (SMEs) improve their security posture.

Generate a clear, structured, and accessible feedback report based on the following assessment data. Your audience is SME business leaders who may not be technical, so use plain language and actionable advice.

Use the following format:

Cyber Hygiene Score
14.71%
Severe: Immediate and decisive cybersecurity action is required.

Introduction
Write a short paragraph summarizing the organization's current cybersecurity hygiene based on the score. Mention whether it's strong, moderate, or weak, and emphasize the importance of continuous improvement.

What You're Doing Well
Highlight areas where the organization is following good practices. Use bullet points and explain why each practice is important.

- Good practice: Do employees have access only to the data and systems required for their job roles (least privilege principle)?
- Good practice: How frequently are data backups performed?

Areas to Improve
Break down weaknesses by category. Clearly explain what needs improvement and why it matters. Use plain language.

Identity & Access Management
- Needs improvement: Do you enforce multi-factor authentication (MFA) for all critical systems (e.g., email, financial software, customer databases)?
- Needs improvement: How often are user access privileges reviewed?
- Needs improvement: Are strong password policies enforced (length, complexity, expiration, reuse restrictions)?
- Needs improvement: Are inactive or terminated employee accounts deactivated immediately?
- Needs improvement: Does your organization provide and require the use of password managers?

Software & Patch Management
- Needs improvement: Does your organization have a centralized system for managing software updates?
- Needs improvement: Do you perform regular vulnerability scans?
- Needs improvement: Are antivirus and endpoint protection solutions installed and updated?
- Needs improvement: How often are operating systems, software, and applications updated?

Data Classification & Protection
- Needs improvement: Does your organization have a formal data classification policy (e.g., Do you inventory and restrict access to sensitive data?)?
- Needs improvement: Are sensitive files and communications encrypted at rest and in transit?

Backup & Recovery
- Needs improvement: Do you have a data backup and recovery process?
- Needs improvement: Are backups stored securely in an offsite or cloud location?
- Needs improvement: Are backups regularly tested for successful restoration?

Security Awareness & Training
- Needs improvement: How often do employees receive cybersecurity awareness training?
- Needs improvement: Are simulated phishing attacks conducted to test employee awareness?
- Needs improvement: Do employees receive role-specific cybersecurity training?
- Needs improvement: Do employees know how to report security incidents and suspicious activity?
- Needs improvement: Do employees understand and actively participate in cybersecurity practices (e.g., reporting suspicious activity, following policies)?

Network & Endpoint Security
- Needs improvement: Does your organization enforce secure Wi-Fi policies (e.g., WPA3, no default credentials, guest network separation)?
- Needs improvement: Are all devices protected with endpoint security solutions (e.g., EDR, antivirus, firewalls)?
- Needs improvement: How is remote access to company systems secured?

Incident Response & Business Continuity
- Needs improvement: Does your organization have a documented incident response plan?
- Needs improvement: Do you have a cybersecurity expert or service provider to help during emergencies (e.g., ransomware, data breaches)?
- Needs improvement: Are security incidents logged and analyzed for patterns?
- Needs improvement: Is there a cyber insurance policy to mitigate financial losses from cyber incidents?
- Needs improvement: How quickly are cybersecurity incidents required to be reported internally?

Compliance & Regulatory Alignment
- Needs improvement: Does your organization follow industry-specific cybersecurity regulations or standards (e.g., ISO 27001, E-ITS, NIS2)?
- Needs improvement: Are third-party vendors required to meet cybersecurity standards?

Physical Security
- Needs improvement: Are devices (laptops, servers, etc.) physically secured against unauthorized access?

Third-Party Risk
- Needs improvement: Do you assess vendors/partners for cybersecurity practices before sharing data or system access?

Remote Work Security
- Needs improvement: Are employees required to use VPNs or secure networks when accessing company data remotely?

Potential Risks and Risk Scenarios
Based on the findings above, identify potential risks and describe them in short, scenario-based statements (e.g., “Without MFA, an attacker could take over email accounts.”).

Action Plan
Provide a prioritized and **concrete cybersecurity action plan** for the organization based on the findings above. Break actions into timeframes based on effort and urgency. Ensure **each timeframe has at least 4–6 specific, actionable tasks** the organization can execute. Where helpful, briefly suggest how to get started with each step (e.g., what tools, resources, or internal processes to explore).

Immediate (0–30 Days)
These should be quick wins or critical issues. Phrase them as direct, clear steps.

Short-Term (60–90 Days)
Mid-term improvements requiring some planning.

Medium-Term (3–6 Months)
Strategic actions for sustained cybersecurity maturity.

Conclusion
Encourage the organization to continue improving its cybersecurity posture. Recommend reassessing in 6–12 months. Reinforce that even small steps can significantly reduce risk.

Return the feedback as if you were delivering it to a real SME client.