Organization Feedback:

Overall Organization Cyber Hygiene Score: 73.61% (Moderate Risk – Immediate improvements recommended in key areas)
Executive Summary
■ **Overall Cyber Hygiene Score:** 73.61% (Moderate Risk)
Key Findings:
■ **Incident Response & Reporting: 0.00% - Immediate improvements needed.**
■ **Secure Communication & Remote Work: 0.00% - Immediate improvements needed.**
Top Priorities:
1■■ **Implement multi-factor authentication (MFA) for all critical accounts (30 days).**
2■■ **Increase phishing simulation frequency to quarterly (45 days).**
3■■ **Enforce end-to-end encryption for all sensitive data (60 days).**
Access Management & Authentication
Score: 93.75%
Access Management & Authentication
■ **Moderate-Risk Areas:**
Assessment of Current Security Posture for 'Do you enforce multi-factor authentication (MFA) for all critical systems?':
Score: 3
Response 3 indicates a need for improvement.
Identified Weaknesses & Risks:
Security measures are in place, but gaps remain that could be mitigated with stronger policies and oversight.
Recommended Improvements:
1. Review and update access controls regularly within 60 days.
2. Perform regular vulnerability assessments within 60 days.
3. Enhance data encryption practices within 90 days.
Priority Level: **Moderate – Address within 60 days**
Assessment of Current Security Posture for 'How often are user access privileges reviewed?':
Score: 3
Response 3 indicates a need for improvement.
Identified Weaknesses & Risks:
Security measures are in place, but gaps remain that could be mitigated with stronger policies and oversight.
Recommended Improvements:

1. Review and update access controls regularly within 60 days.
2. Perform regular vulnerability assessments within 60 days.
3. Enhance data encryption practices within 90 days.
Priority Level: **Moderate – Address within 60 days**
Employee Awareness & Training
Score: 100.00%
Employee Awareness & Training
■ **Low-Risk Areas:**
Assessment of Current Security Posture for 'How often do employees receive cybersecurity awareness training?':
Score: 4
Response 4 suggests strong practices are in place.
Identified Weaknesses & Risks:
Minimal risks detected, but continuous monitoring is advised.
Recommended Improvements:
1. Maintain current practices and conduct regular audits within 90 days.
2. Stay updated with the latest cybersecurity trends within 90 days.
3. Encourage a culture of continuous improvement within 90 days.
Priority Level: **Low Priority – Maintain best practices**
Incident Response & Reporting
Score: 0.00%
Incident Response & Reporting
Secure Communication & Remote Work
Score: 0.00%
Secure Communication & Remote Work