

Unified Feedback

Cybersecurity Assessment Feedback for [SME Name]

Dear [SME Name] Team,

Thank you for the opportunity to conduct this cybersecurity assessment. We appreciate your commitment to strengthening your organization's cybersecurity posture. Your unified score of 50.00% reflects a solid foundation, but as outlined, there are critical areas that need further development for robust security.

Strengths Identified:

- **Organizational and Employee Alignment:** Both organizational and employee scores are at 50.00%, indicating that there is a cohesive effort towards achieving cybersecurity objectives. This is an excellent starting point for developing a comprehensive cybersecurity strategy.

Key Areas for Improvement:

1. **Policy and Practice Alignment:** There currently exists a gap between your established cybersecurity policies and their practical implementation. Ensuring that what is outlined in your documentation is mirrored in daily activities is crucial.
2. **Communication and Training:** Greater emphasis on communication and continuous training is necessary. Employees need to be regularly informed and educated on the evolving landscape of cybersecurity threats.

Potential Risks:

- **Misalignment Risks:** The existing misalignment between policies and real-world employee behavior could lead to vulnerabilities.
- **Inconsistency Across Teams:** Varying security practices across different teams could lead to uneven protection levels and potential exposure.

Action Plan:

Immediate Actions (0–30 Days):

- **Clear Communication of Policies:** Develop and distribute clear and accessible documentation of your cybersecurity policies. Engage with team leaders to ensure the message reaches all employees effectively.
- **Mandatory Security Training:** Ensure that all employees participate in comprehensive security training sessions. This will help everyone understand the importance of cybersecurity and their role

within it.

- **Access Control and Onboarding Review:** Audit the current access controls to ensure they are appropriate for each role. Tighten onboarding processes to reinforce security from the first day an employee joins.

Short-Term Goals (60–90 Days):

- **Policy and Practice Workshops:** Conduct interactive workshops aimed at bridging the gap between policy and practice. Involve employees from various departments to share insights and foster a shared understanding.
- **Monitoring and Reinforcement:** Implement mechanisms to monitor security practices actively. Use this data to reinforce positive behavior and adjust policies as necessary.

We understand the challenges you face and are here to support you every step of the way. By focusing on these immediate actions and short-term goals, your organization can enhance security and minimize risks effectively. Collaboration and communication are key, and we are dedicated to helping you build a secure and resilient infrastructure for the future.

If you have any questions or need further assistance, please feel free to reach out.

Best regards,

[Your Name]

[Your Position]

[Your Contact Information]