Date: [Insert Date]

To: Board of Directors and Executive Management
From: [Insert Name/Title of Information Security Officer or Auditor]
Subject: Annual Penetration Testing Posture Supervisory Letter

1. Executive Summary

This letter summarizes the results and security posture resulting from the annual penetration testing program conducted for the fiscal year [Insert Year]. The purpose of this assessment was to identify vulnerabilities, evaluate the effectiveness of current security controls, and ensure compliance with regulatory requirements.

2. Scope of Assessment

The testing included the following environments:

- External Network Infrastructure (Internet-facing assets)
- Internal Network Infrastructure (Lateral movement and privilege escalation)
- Web Applications (Customer portals and internal APIs)
- [Optional: Wireless Networks / Social Engineering / Physical Security]

3. Methodology

Testing was performed by [Internal Team Name / Third-Party Vendor Name] using a [Black Box / Grey Box / White Box] approach. The methodology followed industry standards such as OWASP and PTES to simulate real-world cyber-attack scenarios.

4. Key Findings and Risk Distribution

The assessment identified the following number of vulnerabilities categorized by severity:

- Critical: [Number]
- High: [Number]
- Medium: [Number]
- Low/Informational: [Number]

5. Remediation Status

As of the date of this letter, the remediation status is as follows:

- **Resolved:** [Number] vulnerabilities have been fully patched and verified.
- **In Progress:** [Number] vulnerabilities are currently being addressed within the defined SLA.
- **Risk Accepted:** [Number] vulnerabilities have been formally documented and accepted by management due to [Reason].

6. Overall Security Posture

The overall security posture of the organization is currently rated as [Satisfactory / Needs Improvement / Unsatisfactory]. Compared to the previous year, the organization has shown [Improvement / Stability / Decline] in its ability to detect and respond to simulated threats.

7. Recommendations

Management should prioritize the following actions over the next quarter:

- [Recommendation 1]
- [Recommendation 2]
- [Recommendation 3]

8. Conclusion

Continuous monitoring and regular testing remain vital to protecting the organization's information assets. A full detailed report is available upon request for authorized stakeholders.

Signature:

_____
[Insert Name]
[Insert Title]
[Insert Department]