

Date: [Insert Date]

To: The Board of Directors and Audit Committee

From: [CISO Name], Chief Information Security Officer

Subject: Annual Cybersecurity Program Attestation - Fiscal Year [Year]

Dear Members of the Board,

As the Chief Information Security Officer of [Company Name], I am providing this formal attestation regarding the status and effectiveness of our Information Security Program for the period ending [Date].

1. Compliance and Governance

I certify that the Information Security Program is designed to comply with applicable laws, regulations, and industry standards, including [List Standards, e.g., NIST CSF, ISO 27001, GDPR]. The program is governed by approved policies that are reviewed and updated annually.

2. Risk Management

We have conducted comprehensive risk assessments to identify, evaluate, and mitigate threats to our information assets. Residual risks have been documented and communicated to the appropriate executive leadership.

3. Program Effectiveness

Based on internal audits, vulnerability assessments, and third-party penetration testing, I attest that the controls currently in place are operating with [Effective/Marginal/Developing] maturity. Key performance indicators (KPIs) and security metrics are tracked to ensure continuous improvement.

4. Incident Response

The organization maintains an active Incident Response Plan. We have conducted [Number] tabletop exercises this year to ensure readiness. All significant security incidents during this period have been reported to the Board in a timely manner.

5. Conclusion

To the best of my knowledge, the Information Security Program provides reasonable assurance that the organization's data and infrastructure are protected against unauthorized access, disclosure, and disruption.

Sincerely,

[CISO Name]
Chief Information Security Officer
[Company Name]

Acknowledged by:

[Name of Board Chair/Audit Committee Chair]

Date: [Insert Date]