Vendor Risk Assessment – Executive Summary

This executive summary provides an overview of the Vendor Risk Assessment performed against a critical SaaS provider. The goal of this assessment was to evaluate the vendor's security posture, compliance certifications, and incident response readiness. Findings were prioritized using a risk scoring model (likelihood × impact).

Risk Heatmap

	Low Impact	Medium Impact	High Impact
Low Likelihood	Low	Low-Medium	Medium
Medium Likelihood	Low-Medium	Medium	High
High Likelihood	Medium	High	Critical

Key Findings

1. Vendor lacks SOC 2 Type II certification (High Risk).
2. Vendor encryption supported only TLS 1.0, requiring remediation (High Risk).
3. No evidence of annual penetration testing (Medium Risk).
4. Incident response plan documented, but untested (Medium Risk).

Recommendations

* Require vendor to achieve SOC 2 Type II within 12 months.
* Enforce upgrade to TLS 1.2+ for all encrypted communications.
* Mandate independent penetration testing annually.
* Conduct joint tabletop exercises to validate incident response readiness.

This vendor risk assessment identified critical gaps that require remediation before contract execution. With compensating controls and a structured POA&M;, the vendor can align with enterprise security standards and reduce overall third-party risk exposure.