Analysis Risk Ratings

This document is applicable to SOC Analyses, Business Continuity Analyses, Cybersecurity Analyses, Information Security and Privacy Assessments, Privacy Analyses, CAIQ Analysis, and Regulatory Compliance and Operational Analyses.

Confident / Low	Vendor appears to maintain a well-formed control environment. Unanswered, unchecked, and unmitigated items should be internally assessed, then accepted or mitigated. Responses appear appropriate.	**Cautious / High**	Vendor does not appear to maintain, or has provided insufficient evidence of, a well-formed control environment. Unanswered, unchecked, and unmitigated items should be internally assessed, then accepted or mitigated. Responses appear insufficient and/or introduce a cautionary level of risk.
Satisfactory / Medium	Vendor appears to maintain a partially well-formed control environment. Unanswered, unchecked, and unmitigated items should be internally assessed, then accepted or mitigated. Responses appear satisfactory.	**Vulnerable / Severe**	Vendor does not appear to maintain, or has provided insufficient evidence of, a well-formed control environment. Unanswered, unchecked, and unmitigated items should be internally assessed, then accepted or mitigated. Responses appear insufficient and/or introduce a severe level of risk.

DETERMINATION OF RISK RATINGS

While analyzing the evidence provided, Venminder summarizes the information within the analysis' individual sections. Each data point within the sections is assigned a point value. Some point values can be adjusted consistently across vendors to reflect context, such as mentioned versus tested controls in a SOC report or supported versus unsupported answers for any other analyses. The individual sections are then rated, which are then used as input for the analysis' overall rating. Professional judgement is used by our Information Security Team, where appropriate, while assigning ratings, determining whether context warrants a higher or lower risk rating than the scoring shows alone.

CONFIDENT/LOW RISK

Upon evaluation of the provided documentation, the vendor appears to maintain a well-formed and well-executed control environment per the scope of the analysis or System and Organization Controls (SOC) report. Appropriate controls, determined by Venminder's Information Security Team within the scope of the analysis, were identified and evaluated. Venminder may have recommendations to evaluate certain items further, but no special action appears necessary, unless there are critical subservice organizations which have not been reviewed.

SATISFACTORY/MEDIUM RISK

Upon evaluation of the provided documentation, the vendor appears to maintain an adequate and stable control environment per the scope of the analysis or SOC report. Controls were identified and evaluated, but additional interaction with the vendor to discuss controls and topics not covered, or found to be deficient by provided documentation, is recommended.

CAUTIOUS/HIGH RISK

Upon evaluation of the provided documentation, the vendor appears to introduce an elevated level of uncertainty, either due to an insufficient amount of information provided and/or process findings or deficiencies. Due to this, remediation of the items introducing uncertainty is recommended and follow-up action should include additional analysis.

VULNERABLE/SEVERE RISK

Upon evaluation of the provided documentation, the vendor appears to introduce a high level of uncertainty, either due to an insufficient amount of information provided and/or process findings or deficiencies. Due to this, remediation of the items introducing uncertainty is recommended and follow up action should include additional analysis.