Third-Party Risk Assessment Report

Zoom Video Communications Inc.

Prepared by: Wael Rezgui
Date: July 26, 2025

1. Objective

This report aims to provide a comprehensive third-party security risk assessment of Zoom Video Communications Inc., focusing on evaluating their security posture, compliance with industry standards, and potential risks associated with using their services. The intent is to inform decision-makers about Zoom's suitability as a vendor for handling sensitive data and critical communications.

2. Scope

This assessment covers Zoom's core video conferencing and collaboration services, including data encryption practices, authentication controls, compliance certifications, incident history, and contractual protections relevant to data privacy and security. The evaluation uses publicly available information as of the date of this report.

3. Assumptions & Limitations

- All information is sourced from publicly available Zoom documentation, trust centers, and security reports.
- Internal policies or configurations within client organizations are not assessed.
- This report does not replace a full technical audit or penetration test of Zoom's systems.
- Risk scoring is based on standardized questionnaires and may not cover all specific organizational risk appetites.

4. Methodology

- Reviewed Zoom's official security whitepapers, compliance certifications, and trust center documents.
- Developed a security questionnaire aligned with industry best practices and standards (ISO 27001, SOC 2, GDPR).
- Assigned risk scores to each control based on Zoom's documented compliance or response.
- Analyzed risk scores to derive an overall risk rating and identified key observations.

5. Vendor Overview

Name: Zoom Video Communications Inc.
Headquarters: San Jose, California, USA

Services: Video Conferencing, Webinars, Chat, Cloud Phone Systems, and Collaboration Tools
Customers: Individual users, Enterprises, Educational Institutions, Healthcare Providers
Data Sensitivity: Medium to High (may include PII, PHI, confidential business data)
Use Case Examples: Internal meetings, external communications, training sessions, telehealth, webinars

6. Security Questionnaire & Risk Scoring

The following table summarizes Zoom's adherence to critical security controls relevant to third-party risk management. Scoring: 1 = Fully compliant/passed, 0.5 = Partially compliant, 0 = Non-compliant or unknown.

#	Control / Question	Zoom's Response	Score
1	Data encryption at rest	Data encrypted using AES-256 standards across all storage locations.	1
2	Data encryption in transit	TLS 1.2+ encryption for all data traversing networks, including meetings.	1
3	Multi-Factor Authentication (MFA) for user and admin accounts	MFA is supported and recommended; enforced on admin accounts.	1
4	Holds ISO 27001 and SOC 2 Type II certifications	Both certifications are current and publicly validated.	1
5	Regular penetration testing and vulnerability assessments	Conducted quarterly by third parties; remediation tracked.	1
6	Regional data residency options	Customers may select data storage regions in select plans.	1
7	Data deletion upon request and retention policies	Data deletion mechanisms comply with GDPR and CCPA.	1
8	Administrative access logging and audit trails	Comprehensive logs maintained and monitored.	1
9	Signed Data Processing Agreement (DPA) availability	Standard DPAs provided with contractual agreements.	1
10	History of major security incidents	Zoom-bombing incidents in 2020 mitigated promptly with fixes and security enhancements.	0.5

Table 1: Security Controls and Risk Scoring for Zoom

7. Risk Summary

Vendor	Total Score	Risk Level	Comments
Zoom	9.5 / 10	Low Risk	Zoom has demonstrated strong remediation capabilities and maintains industry-standard controls. Past incidents were quickly mitigated.

Table 2: Overall Risk Rating

8. Observations

- Zoom's commitment to compliance is evidenced by multiple certifications (ISO 27001, SOC 2).
- Encryption practices follow best-in-class standards ensuring confidentiality.
- Incident response improved substantially post-2020, with a focus on user security.
- Regional data residency options enable clients to meet data sovereignty requirements.
- Some residual risk exists due to the 2020 breach history, but mitigations appear sufficient.

9. Recommendations

- Ensure enterprise contracts include detailed SLAs, DPAs, and data handling terms tailored to organizational policies.
- Implement and enforce MFA across all user and administrator accounts.
- Monitor Zoom's security advisories and update configurations regularly.
- Conduct periodic reviews of Zoom's compliance status and incident history.
- If handling highly sensitive or regulated data, consider additional encryption or compensation controls.

10. Glossary

ISO 27001: International standard for information security management systems.

SOC 2: Service Organization Control 2 — report on controls relevant to security, availability, processing integrity, confidentiality, and privacy.

MFA: Multi-Factor Authentication, an additional security layer requiring multiple verification methods.

DPA: Data Processing Agreement, a contract outlining how data is processed by the vendor.

Zoom-bombing: Unauthorized intrusion into Zoom meetings.

This report is a simulated security assessment created for educational and portfolio purposes. All data is publicly available as of the date of writing.