Prompt:

You are a cybersecurity analyst reviewing vendor security documentation for a Global Vendor Security Assessment (VSA). Your task is to analyze all provided documents and generate a comprehensive risk assessment.

VENDOR INFORMATION:

- Vendor Name: [Vendor Name]
- Primary Domain: [Domain]
- Products/Services: [Product List]

DOCUMENTS PROVIDED:

[List of documents with types and dates]

ANALYSIS REQUIREMENTS:

1. CONTROL INVENTORY

Extract and categorize all security controls mentioned in the documents according to these categories:

- Organization & Governance
- Certifications & Compliance
- Access Control & Authentication
- Data Protection
- Security Operations
- Vendor & Supply Chain Management
- Business Continuity & Resilience
- Security Training & Awareness
- Physical & Environmental Security
- Incident History & Breach Response

For each control, provide:

- Control description
- Implementation status (Implemented/Partially Implemented/Not Implemented/Unknown)
- Evidence from documents (with specific page/section citations)
- Effectiveness assessment (if testing results available)
- Last validation date (if available)

2. REQUIREMENTS MAPPING

Compare extracted controls against these mandatory requirements:

- SOC 2 Type II report (current within 12 months)
- ISO 27001 or equivalent certification
- MFA for administrative access
- Encryption at rest and in transit
- Documented incident response plan
- Third-party risk management program
- Annual security training
- Penetration testing (within 12 months)
- Business continuity/disaster recovery plan

For each requirement, indicate: MET / PARTIALLY MET / NOT MET / INSUFFICIENT INFORMATION

3. RISK ASSESSMENT

Based on the analysis, provide:

- Overall Risk Rating: LOW / MEDIUM / HIGH / CRITICAL
- Confidence Level: [0-100%] - how confident are you in this assessment based on document completeness
- Key Strengths: [List 3-5 notable security strengths]
- Key Weaknesses: [List 3-5 security gaps or concerns]
- Missing Information: [List critical information not found in documents]
- Red Flags: [List any serious concerns requiring immediate SE attention]

4. SECURITYSCORECARD CORRELATION

Based on the documentation, predict likely SecurityScorecard issue areas:

- Email security (SPF/DKIM/DMARC/TLS)
- Patching cadence
- Network security
- Application security
- Endpoint security

5. ENDORSEMENT RECOMMENDATION

Provide preliminary recommendation:

- RECOMMEND ENDORSEMENT: All mandatory requirements met, no critical concerns
- CONDITIONAL ENDORSEMENT: Minor gaps exist, recommend with conditions
- ADDITIONAL REVIEW REQUIRED: Significant gaps or concerns need SE investigation
- RECOMMEND REJECTION: Critical requirements not met or serious security concerns

6. SE REVIEW PRIORITIES

Highlight specific areas requiring detailed SE review:

[List specific sections, findings, or concerns]

OUTPUT FORMAT:

Provide analysis in structured markdown format with clear sections and subsections. Use tables where appropriate for control inventories and requirement mappings. Include specific page numbers and document names for all evidence citations.

CRITICAL: Base all findings strictly on evidence in the provided documents. If information is not available, explicitly state "Insufficient Information" rather than making assumptions. Cite specific document names and page/section numbers for all findings.

Examples:

Full Review of - based on 27 documents from the Trust Center.

Global Vendor Security Assessment: NotYourCompany

Assessment Date: January 16, 2026

Vendor Name: NotYourCompany, PBC

Primary Domain: NotYourCompany.com

1. Control Inventory

Category	Control Description	Status	Effectiveness Assessment	Last Validation
Organization & Governance	Executive Risk Council (ERC) oversees internal controls and meets quarterly to align strategy.	Implemented	Effective; reviews show quarterly meetings were held.	Sept 30, 2025
Certifications & Compliance	ISO/IEC 27001:2022 Certification for the ISMS supporting AI services.	Implemented	Validated by accredited third-party registrar.	Nov 13, 2025
Access Control	MFA enforced via hardware tokens; zero-trust model used for network access.	Implemented	Effective; verified in configuration testing.	Sept 30, 2025

Access Control	Quarterly privileged access reviews to ensure roles remain commensurate.	**Partially Implemented**	**Exception**: One quarterly review was missed due to personnel changes.	Sept 30, 2025
Data Protection	AES-256 encryption at rest; TLS 1.2+ for data in transit.	Implemented	Effective; verified in system configurations.	Sept 30, 2025
Security Operations	Continuous vulnerability scanning, red teaming, and annual 3rd-party penetration tests.	Implemented	Effective; multiple independent assessments performed.	July 2025
Vendor Management	Due diligence program including annual review of subservice provider SOC reports.	Implemented	Effective; management performed annual reviews of GCP/AWS.	Sept 30, 2025
BCDR	Daily automated backups with 30-day retention; annual disaster recovery plan testing.	Implemented	Effective; annual recovery exercise completed.	Sept 30, 2025
Security Training	Mandatory security and privacy awareness training upon hire and annually.	Implemented	Effective; verified through employee training records.	Sept 30, 2025

Physical Security	Physical access restricted via subservice data centers with NotYourCompany monitoring.	Implemented	Effective; managed via shared responsibility model.	Sept 30, 2025
Incident Response	Incident Response program with escalation tiers and annual tabletop exercises.	Implemented	Effective; procedures tested and updated annually.	Sept 30, 2025

2. Requirements Mapping

Mandatory Requirement	Status	Summary
SOC 2 Type II Report	**MET**	Current report covers the period ending Sept 30, 2025.
ISO 27001 Certification	**MET**	ISO/IEC 27001:2022 certified through Jan 6, 2028.
MFA for Admin Access	**MET**	Enforced for cloud consoles, applications, and internal resources.
Encryption (Rest/Transit)	**MET**	Implemented using industry-standard AES-256 and TLS protocols.
Incident Response Plan	**MET**	Documented plan exists and is validated via annual testing.
Third-Party Risk Program	**MET**	Formal vendor onboarding and annual monitoring in place.
Annual Security Training	**MET**	Verified for all employees including privacy-specific modules.
Penetration Testing	**MET**	Multiple assessments (Network, Web, API, Client) completed in 2025.
BCDR Plan	**MET**	Verified DR plan with established recovery time objectives.

3. Risk Assessment

- **Overall Risk Rating: LOW**
- **Confidence Level: 95%**
- **Key Strengths:**
  - Dual-layer validation through a clean SOC 2 Type II (notwithstanding one exception) and active ISO 27001 certification.
  - Highly automated infrastructure security, specifically the "ephemeral node" strategy that ensures servers are always patched and fresh.
  - Wide-ranging penetration testing program that covers the entire ecosystem, including web, API, and native desktop/mobile clients.
- **Key Weaknesses:**
  - **Access Review Failure**: Management failed to conduct one required quarterly access review, which is a key control for preventing privilege creep.
  - **Open Vulnerabilities**: As of the last report update, six "Low" severity findings from 2025 tests remain open with a late 2025 remediation target.
- **Missing Information:**
  - Verification of the actual remediation of the November 2025 open pentest items.
  - Detailed technical descriptions of the specific vulnerabilities identified during pentests (summaries only provided).
- **Red Flags:**
  - No major red flags. The identified access review failure was attributed to a specific staff departure and has a documented remediation plan in place.

4. SecurityScorecard Correlation

- **Email Security:** High performance expected due to centralized Google Workspace and Cloudflare management.

- **Patching Cadence:** Exceptional performance predicted; serverless orchestration and ephemeral instances minimize the window for unpatched software.

- **Network Security:** Robust; reliance on zero-trust tools like Tailscale and Cloudflare WAF indicates a limited external attack surface.

- **Application Security:** Strong; independent assessors noted robust input validation and effective authorization checks across organization boundaries.

- **Endpoint Security:** High; MDM enforcement of FileVault encryption and CrowdStrike agents across the fleet.

5. Endorsement Recommendation

CONDITIONAL ENDORSEMENT

NotYourCompany demonstrates a mature and transparent security posture that meets all standard corporate requirements. The recommendation is conditional on the following:

1. Verify that the newly implemented "runbooks" for access reviews are being followed to prevent another missed review.
2. Request a status update confirming that the findings with the November 28, 2025, target date were closed as planned.

6. SE Review Priorities

- **Access Review Remediation**: Confirm that logical access reviews have resumed their quarterly cadence and that cross-training has successfully removed the "single point of failure" regarding personnel.
- **Pentest Follow-up**: Review finding IDs 2124297 through 2124301 to ensure they have been moved to "Closed" status.
- **Service Dependency**: Review the SOC report's description of subservice organization controls (GCP/AWS) to ensure NotYourCompany's assumptions about infrastructure security align with internal risk appetite.