MEMORANDUM

TO: Investment Committee & Risk Management Group, Meridian Wealth Partners
FROM: Carolina Pinto, GRC Analyst
DATE: August 14, 2026
SUBJECT: Third-Party Vendor Risk Evaluation — ClientVantage CRM Renewal
REF: GLBA Safeguards Rule / SEC Cybersecurity Risk Oversight Guidelines

1. Executive Summary & Context

Meridian Wealth Partners ("Meridian") currently engages ClientVantage Technologies, Inc. ("ClientVantage") for SaaS-based client relationship management, secure document hosting, and client portal operations. As the platform holds ultra-high-net-worth (UHNW) non-public personal information (NPI), financial account details, and KYC/AML documentation, a formal vendor risk evaluation was conducted ahead of upcoming contract renewal negotiations.

Based on control design review, SOC 2 Type II audit report analysis, and vendor questionnaire responses, ClientVantage exhibits a Medium-High risk profile (weighted score 2.95 / 5.00). While the vendor maintains a mature baseline security framework and an unqualified SOC 2 Type II audit, the report identified two control exceptions concerning access review timelines and encryption key rotation.

Renewal is recommended, subject to mandatory contractual addenda including a strict 48-hour breach notification requirement, right-to-audit remedies for audit exceptions, and minimum cyber insurance verification.

2. Operational Profile & Data Architecture

Vendor Entity	ClientVantage Technologies, Inc. (ClientVantage CRM)
Service Scope	Multi-tenant SaaS client portal & wealth CRM
Hosting Infrastructure	AWS us-east-1 (SOC 2 & ISO 27001 certified underlying)
Data Handled	Client PII/NPI, financial account details, KYC/AML records, tax IDs
Internal Users	~45 Meridian personnel (advisors, compliance, operations)
Business Criticality	High — core operational platform & primary client portal
Fourth-Party Vendors	AWS (hosting), SendGrid (transactional email), Twilio (SMS MFA)

Data Transmission Summary: Authentication occurs via SAML 2.0 SSO enforced by mandatory MFA. Transits utilize TLS 1.2+ encryption, with storage in AWS RDS encrypted at rest (AES-256). Nightly API

batch syncs with Meridian's internal portfolio engine utilize authenticated REST APIs with quarterly key rotation schedules.

3. Control Assessment & Questionnaire Findings

- **Access Controls & Identity Management:** Role-based access control (RBAC) is implemented at the tenant level. Multi-factor authentication is enforced for all administrative and standard user accounts.
- **Data Protection & Encryption:** AES-256 encryption is applied at rest; TLS 1.2+ is enforced in transit. Production data remains strictly within AWS us-east-1 without cross-region replication.
- **Vulnerability & Incident Management:** Independent annual third-party penetration testing is performed. SLA mandates remediation of critical vulnerabilities within 15 days. Incident response playbooks are tested annually via tabletop exercise.
- **Data Retention & Offboarding:** Contract termination terms stipulate a 90-day retention window followed by permanent cryptographic erasure and issuance of a formal Certificate of Deletion.

4. SOC 2 Type II Audit Review

Audit Period: June 1, 2025 – May 31, 2026 | Auditor: Harbridge & Associates LLP | Opinion: Unqualified (with exceptions)

The independent CPA audit verified control suitability across Security, Availability, and Confidentiality. Two specific operational exceptions were noted in the report:

- **Access Review Cadence Delay:** One quarterly user access review was completed 19 days past the vendor's internal SLA. Corrective Action: Automated administrative workflow reminders were instituted mid-period.
- **Encryption Key Rotation Interval:** Encryption key rotation for a secondary subsystem was executed on an 18-month cycle rather than the vendor's documented 12-month policy. Auditor verified no evidence of key compromise.

Assessment Team Guidance: While neither exception represents an active security breach, delayed access reviews directly touch Meridian's regulatory duties under the GLBA Safeguards Rule. Meridian should require written proof of remediation prior to the next annual review.

5. Risk Scoring & Quantification

Risk Domain	Score (1-5)	Weight	Weighted	Rationale / Notes
Data Sensitivity	4	25%	1.00	Regulated PII, financial, and KYC records
Access Scope	3	15%	0.45	Broad internal user base with RBAC enabled
Control Maturity	2	20%	0.40	Strong baseline; two SOC 2 exceptions

Compliance Posture	3	15%	0.45	SOC 2 Type II current; ISO 27001 pending
Business Continuity	2	10%	0.20	Tested RTO (4h) and RPO (1h)
Subprocessor Exposure	3	15%	0.45	Reputable hosting/SMS subprocessors
TOTAL WEIGHTED SCORE		**100%**	**2.95**	**Medium-High Risk Classification**

6. Mandatory Contractual Terms for Renewal

To align the engagement with Meridian's legal and regulatory obligations, contract renewal must incorporate the following terms:

- **Firm 48-Hour Incident Notification:** Replace current 'without undue delay' language with a strict contractual obligation to notify Meridian within 48 hours of confirming a security incident.
- **Right-to-Audit & Exception Remediation:** Retain Meridian's right to request written proof of remediation for all SOC 2 audit exceptions at each renewal cycle.
- **Subprocessor Advance Notice:** Require at least 30 days' advance written notice prior to onboarding or replacing fourth-party subprocessors with data access.
- **Cyber Insurance Minimums:** Mandate proof of cyber liability coverage of at least $2M per occurrence.
- **Annual SOC 2 Delivery SLA:** Require automatic delivery of updated annual SOC 2 Type II reports within 30 days of issuance.

7. Final Recommendation

Action Requested: APPROVE RENEWAL WITH CONDITIONS.

ClientVantage CRM demonstrates acceptable technical control maturity to remain Meridian's CRM and portal provider. However, approval should remain contingent upon executing the contractual addenda detailed in Section 6. Compliance will track exception remediation during the August 2027 review cycle.