# ChatGPT Response

Rating Summary

• Inherent Risk: High

• Justification: Vendor hosts and processes sensitive customer data (incl. PCI/HIPAA use cases) in cloud databases; has privileged DBA access to client environments; depends on multiple subservice providers (Microsoft Azure, Logicworks, Alert Logic). Business impact of compromise would be significant.

• Control Effectiveness: Partially Effective (~72%)

• Evidence:

• Strong hosting controls evidenced by current unqualified SOC 2 Type 2 reports for Microsoft Azure (Security/Availability/PI/Confidentiality; minor, remediated exceptions) and Logicworks (Security/Availability/Confidentiality).

• Internal policies cover many domains (NIST 800‑30/39/61/63; AES‑256 at rest, TLS 1.2 in transit; SSO/MFA; annual risk assessments).

• But security questionnaire shows material gaps in governance (no designated CISO; no formal risk treatment program), network/device hardening/logging, mobile/MDM, application security (no OWASP/SCA/secure reviews), and privacy safeguards.

• Residual Risk: High

• Reasoning: High inherent risk combined with Partially Effective controls → High (per Beaconer Residual Risk Matrix).

Control Testing Metrics

• % Control Coverage: ~72% (SOC 2 hosting controls fully covered; internal program shows notable gaps across multiple domains)

• Total Gaps Identified: 19

• Total Critical Gaps: 5

• Residual Risk Calculation Explanation: High inherent risk (sensitive data, privileged access, subservice reliance) + Partially Effective internal controls (governance/privacy/appsec/network gaps despite strong hosting SOC 2s) = High residual risk.

Control Testing (Domain Example – Access Control)

Control Question Vendor Response Evidence / Notes

Program approved & communicated Yes Bellaire/D3 Information Security Policy; Password Guideline (Sept 2022)

Regular access review for all Yes Security Questionnaire Q41–42 Yes; DBA access reviewed semi‑annually; weekly log review (D3 policy)

IDs are auto terminated on last day Yes Security Questionnaire Q53 Yes; Employee Handbook termination procedures

Segregation of duties Yes Security Questionnaire Q52 Yes; D3 policy mandates SoD

Controls for Corporate Email on personal phones No Q65 Yes but MDM Q284–285 No; lacking enforced MDM/PIN/encryption

MFA deployed Yes D3: SSO with MFA tokens; Questionnaire Q44–45 Yes

Application supports customer SSO Yes Questionnaire Q47 Yes (SAML/SSO)

Unique IDs required Yes Questionnaire Q48 Yes

Principle of least privilege Yes Questionnaire Q50 Yes

Password policy Yes Password Guideline (14+ chars, complexity; 6‑month user/quarterly system change); D3 policy notes 90/30 day cadence (inconsistency)

Process to request approval for Access Yes Questionnaire Q49 Yes

Password sharing prohibited Yes Questionnaire Q56 Yes

Passwords are salted & hashed at storage No D3 policy: passwords “encrypted with AES‑256” (encryption ≠ salted hashing); Password Guideline silent on hashing

Gap Analysis

Domain Issues Identified Severity (High/Medium/Low) Risk Counter Measure

Access Control Conflicting password rotation (90 days vs 6 months); lack of enforced idle logoff; weak BYOD/MDM; password storage encrypted not salted+hashed Medium to High Account compromise; data exposure on lost devices; password database offline cracking Align policy to 90‑day user / 30‑day admin rotation OR universal MFA; enforce session idle timeout; implement enterprise MDM (PIN, encryption, remote wipe, compliance); use salted, slow hash (bcrypt/Argon2) for stored passwords

Cryptographic Controls AES‑256/TLS 1.2 in place; Azure secrets rotation exceptions (remediated) but internal password storage uses encryption instead of hash Medium Offline credential attacks; key management drift Adopt salted hashing for credentials; formalize key/secrets rotation SLAs and evidence

Monitoring/Logging Network device logs “insufficient detail” (Q169 No) Medium Incomplete incident reconstruction Implement syslog/NetFlow; define log content (auth, config, ACL hits); 1‑year retention; central SIEM alerts

Incident Response Program aligned to NIST 800‑61; evidence of tooling Low — Conduct at least annual tabletop; measure MTTA/MTTR; integrate vendor breach notification playbooks

BCP/DR Strong subservice (Azure/Logicworks SOC 2s); internal program “Yes” Low — Ensure third‑party dependency mapping and failover runbooks; test restore RTO/RPO annually

Privacy “Business compliant with safeguards to protect personal data”: No (Q125) Critical Non‑compliance; regulatory penalties Stand up privacy program: data mapping, DPIA where applicable, access controls, DSAR workflow, deletion/retention standards, processor DPAs, training; align to GDPR/CCPA where in scope

Training & Governance No designated CISO (Q13); no formal risk treatment program (Q6) High Lack of accountability; unmanaged risks Appoint CISO (or vCISO); establish ISO‑aligned risk treatment plan with owners, timelines, acceptance criteria; report to leadership quarterly

Network Security No device hardening standards (Q166 No); network logs insufficient (Q169 No); no wireless controls (Q176 No) High Network compromise; lateral movement Adopt CIS Benchmarks for routers/switches/firewalls; centralized logging; network ACL reviews; implement WPA2‑Enterprise/802.1X or disable corporate Wi‑Fi if unused

Application Security No OWASP/Secure coding program (Q192 No); no pre‑prod security reviews (Q207 No); no SCA (Q213 No); clients cannot manage API access (Q196 No) Critical Injection/XSS/SSRF/Supply‑chain risk; API abuse Implement SDLC with OWASP ASVS; mandate SAST/DAST/SCA; threat modeling; pre‑prod security gate; API auth (OAuth2/OIDC), rate‑limits, customer role‑based access; logging

Third‑Party Risk Mgmt No remediation reporting for subcontractors (Q84 No); no third‑party inventory by risk (Q87 No) Medium Cascade risk from vendors Create centralized vendor inventory, tiering; require SOC 2/ISO/pen tests; track issues to closure; right‑to‑audit clauses

Physical Security Many N/A (remote‑first) Low WFM risks Harden work‑from‑home: encrypted disks, screens, locked rooms, shredding guidance; enforce via MDM

Notes and Evidence Highlights

• Hosting/Subservice assurance: Microsoft Azure SOC 2 Type 2 (Security/Availability/PI/Confidentiality; minor exceptions remediated) and Logicworks SOC 2 Type 2 (Security/Availability/Confidentiality; unqualified).

• Policy baselines: Information Security Policy (NIST 800‑30/39 risk mgmt; NIST 800‑61 IR; encryption TLS 1.2/AES‑256), Password Guideline (14+ chars, complexity; rotation intervals), Security Questionnaire (many “Yes,” key “No” gaps listed above).

• Azure exceptions (for awareness): network device password rotation cadence, break‑glass alerting (part‑period), two secrets not rotated per cadence, quota configs for two services — remediated per report; low residual impact.

Residual Risk Statement

Despite robust cloud hosting controls, current internal control gaps in governance (CISO/risk treatment), privacy safeguards, application security, and network hardening/logging increase the likelihood and impact of incidents. Until these are remediated and evidenced, residual risk remains High.

Recommended Immediate Priorities (next 90 days)

1) Appoint CISO / establish formal risk treatment plan (board‑endorsed).

2) Implement MDM for all mobile/BYOD with enforced policies.

3) Stand up AppSec program (OWASP ASVS, SAST/DAST/SCA, pre‑prod security gate).

4) Convert password storage to salted hashing (bcrypt/Argon2); align rotation; enforce idle lock.

5) Create network hardening/logging standards (CIS baselines; centralized logs).

6) Launch privacy program with documented safeguards and DPIA/DSAR handling.

Longer‑Term (next 6–12 months)

• Mature vendor risk management (inventory, tiering, monitoring).

• Annual IR/BCP exercises with metrics.

• Continuous control monitoring and quarterly risk reporting to leadership.