# ChatGPT Response

Rating Summary

• Inherent Risk: High

• Justification: Vendor processes PI/SPI/PII and potentially PHI (privacy questionnaire largely “Yes” to PI/SPI handling, encryption, DSAR, RTBF). Hosts/operates in Microsoft Azure and leverages Logicworks (subservice dependencies). Provides API services and integrates with multiple SaaS. Business-critical environment (cloud infrastructure and security operations).

• Control Effectiveness: Partially Effective (~78%)

• Rationale: Strong baseline controls and policies (InfoSec program, encryption in transit/at rest, access controls, MFA, SOC 2 for Microsoft Azure and Logicworks). However, several notable gaps in risk treatment, data lifecycle, mobile/BYOD, wireless, key management SoD, and others (see Gap Analysis).

• Residual Risk: High

• Reasoning: High Inherent + Partially Effective = High (per Beaconer matrix)

Control Testing Metrics

• % Control Coverage: ~78% (based on questionnaire “Yes” responses across domains, InfoSec policy and SOC 2 scope coverage; estimate given volume of controls and observed gaps)

• Total Gaps Identified: 14

• Total Critical Gaps: 6

• Residual Risk Calculation Explanation: With vendor handling sensitive data and relying on subservice providers, inherent risk is High. While many controls exist (policies, MFA, encryption, access governance, SOC 2-aligned subservices), multiple high-severity gaps remain in foundational areas (e.g., risk treatment program, wireless/MDM, data retention/destruction, password storage practice, encryption key SoD). Thus, Control Effectiveness is Partially Effective, yielding High Residual Risk.

Notes on Evidence Reviewed

• Security Questionnaire (selected responses):

• Risk Treatment Program (Q6): No

• Password unencrypted record prohibition (Q61): No

• Asset return on termination (Q71): No

• Third-party remediation reporting (Q84): No

• Third-party inventory by risk (Q87): No

• Automatic logoff required (Q54): No

• Wireless controls implemented (Q176): No

• BYOD MDM and mobile technical enforcement (Q284, Q285): No

• Client ability to manage API access (Q196): No

• Software Composition Analysis (Q213): No

• Data retention/destruction requirement (Q244): No

• Security safeguards compliance attestation (Privacy Q125): No

• Encryption key mgmt SoD (Q237): No

• Policies/Reports:

• Information Security Policy (Azure hosting, encryption TLS 1.2/AES-256, NIST risk methods, IR NIST 800-61, AV, vulnerability management, DRP with RTO<24h/RPO<1h); Logicworks SOC 2 Type 2 (02/01/22–01/31/23) unqualified; Microsoft Azure SOC 2 Type 2 (04/01/22–03/31/23) unqualified with limited exceptions remediated (break-glass alerting in early period, network device password rotation, secret rotation on sampled items).

Section 3: Control Testing (Domain Example – Access Control)

Control Question | Vendor Response | Evidence / Notes

Program approved & communicated | Yes | Access Control Program (Q39 Yes); InfoSec policy defines roles/responsibilities.

Regular access review for all | Yes | Q41 (review access) Yes; Q42 (privileged review) Yes.

IDs are auto terminated on last day | Yes | Q53 Yes (IDs disabled on last day).

Segregation of duties | Yes | Q52 Yes (SoD for granting/approving).

Controls for Corporate Email on personal phones | Yes | Q65 Yes (controls for accessing corp email). Note: BYOD MDM/technical enforcement is No (Q284, Q285).

MFA deployed | Yes | Q44 MFA deployed; Q45 MFA for privileged Yes; InfoSec policy supports.

Application supports customer SSO | Yes | Q47 Yes (SAML/OpenID/SSO available).

Unique IDs required | Yes | Q48 Yes (unique IDs required).

Principle of least privilege | Yes | Q50 Yes (least privilege provisioning).

Password policy | Yes | Q57 complexity minimum 8 and complexity; Password Guideline: user every 6 months; system-level quarterly.

Process to request approval for Access | Yes | Q49 formal request/approval process.

Password sharing prohibited | Yes | Q56 Yes (sharing prohibited).

Passwords are salted & hashed at storage | Yes | Q63 Yes (passwords encrypted/hashed at rest).

Section 4: Gap Analysis

Access Control

Domain | Issues Identified | Severity | Risk | Counter Measure

Access Control | No enforced automatic logoff policy for workstations/sessions (Q54 No) | Medium | Sessions left open increase hijack risk | Enforce inactivity timeouts (e.g., 15 minutes) via GPO/MDM and application session TTL.

Access Control | BYOD without MDM and no technical enforcement (Q284, Q285 No) | High | Data leakage, loss/theft exposure | Deploy MDM/UEM for all mobile endpoints (containerize email, enforce device encryption, PIN, remote wipe); restrict access from unmanaged devices.

Access Control | Corporate email accessible on personal devices without full technical controls | Medium | Leakage via unmanaged email apps | Move to conditional access + app protection policies (Intune) and block IMAP/POP legacy auth.

Cryptographic Controls

Domain | Issues Identified | Severity | Risk | Counter Measure

Cryptographic Controls | Lack of explicit SoD for key management vs operations (Q237 No) | High | Increased chance of key misuse/compromise | Separate key custodianship from ops; use dedicated KMS/HSM with role-based separation; implement key mgmt policy and dual control.

Cryptographic Controls | Passwords may be recorded unencrypted (Q61 No to prohibition) | High | Catastrophic compromise if stored plaintext | Update policy to explicitly prohibit any unencrypted password storage; deploy secret managers (Vault) and scan repos/drives to find & purge secrets.

Monitoring & Logging

Domain | Issues Identified | Severity | Risk | Counter Measure

Monitoring | “Sufficient detail” in network device logs reported No (Q169 No) | Medium | Incomplete logs hinder incident response | Standardize device logging to include admin actions, config changes, successes/failures; centralize to SIEM; validate via periodic audits.

Monitoring | No wireless controls implemented (Q176 No) | Medium | Rogue APs/traffic unmonitored | If any wireless present, implement WPA2/3-Enterprise, NAC, WIPS; or formally forbid Wi‑Fi and monitor for rogue APs.

Incident Response (IR)

Domain | Issues Identified | Severity | Risk | Counter Measure

IR | Third-party remediation reporting process absent (Q84 No) | Medium | Supplier incidents not tracked to closure | Formalize third-party incident & remediation intake, tracking, and reporting SLAs; integrate into IR plan and vendor management.

IR | Some privacy/security exceptions unresolved (Privacy Q125 No) | High | Noncompliance during incidents | Map administrative/technical/physical safeguards to 800-53/ISO 27001 Annex A; remediate gaps; test IR + privacy breach notification.

BCP/DR

Domain | Issues Identified | Severity | Risk | Counter Measure

BCP/DR | Data retention/destruction requirement absent (Q244 No) | High | Over-retention, legal exposure, breach impact | Implement data classification-based retention schedules; automate deletion; include backups/archives; log destructions.

BCP/DR | Asset return on termination not verified (Q71 No) | Medium | Residual data on devices | Enforce exit checklist, asset tracking, remote wipe verification, certificate of return/destruction.

Privacy

Domain | Issues Identified | Severity | Risk | Counter Measure

Privacy | “Business compliant with safeguards” marked No (Q125 No) | High | Potential regulatory non-compliance | Complete privacy controls program (admin/technical/physical), perform PIA/DPIA, and document safeguard evidence; audit readiness for GDPR/CCPA/HIPAA as applicable.

Privacy | Data location/cross-border notices/process unclear | Medium | Residency and transfer risk | Document data residency, sub-processors (Azure/Logicworks), SCC/DPF adherence; publish data maps; contract updates.

Training & Governance

Domain | Issues Identified | Severity | Risk | Counter Measure

Training | Risk treatment program not in place (Q6 No) | High | Risks remain unmitigated | Stand up risk treatment lifecycle with owners, timelines, acceptance criteria, and board reporting (NIST 800‑39/ISO 27005).

Training | Software Composition Analysis (SCA) not performed (Q213 No) | Medium | Open-source vulnerabilities | Implement SCA (e.g., Snyk, Dependabot) and integrate into CI/CD with policy gates.

Physical & Network Security

Domain | Issues Identified | Severity | Risk | Counter Measure

Physical/Network | Wireless controls not implemented (Q176 No) | High | Unauthorized network access | Either disallow Wi‑Fi or deploy enterprise Wi‑Fi with NAC; monitor with WIPS; network segmentation.

Physical/Network | Separate network segment/dedicated endpoints for remote access—status unclear/partial | Medium | Lateral movement | Ensure jump hosts/bastion with MFA; split-tunnel off; segment admin networks; enforce PAM and session recording.

API & Application Security

Domain | Issues Identified | Severity | Risk | Counter Measure

Application/API | Clients cannot manage access to the APIs (Q196 No) | Medium | Excessive privileges, key sprawl | Provide API key scoping, per-client RBAC/OAuth2; enable rotation/self-service revocation; add rate limiting & logging.

Application | SAST/DAST present but SCA absent (Q213 No) | Medium | Dependency vulns | Add SCA to the secure SDLC; maintain SBOM; remediate CVEs with SLAs.

Additional Observations (Subservice Providers)

• Microsoft Azure SOC 2 Type 2 (04/01/22–03/31/23): Unqualified opinion. Noted exceptions early in period (break-glass alerting on 2 of 4 domains, network device password rotation, select secret rotations), with remediation and comp controls. Strong coverage of Security/Availability/Confidentiality.

• Logicworks SOC 2 Type 2 (02/01/22–01/31/23): Unqualified opinion; controls for Managed Cloud Operations effective. No adverse findings.

Recommended Next Steps (Priority)

1) Establish formal Risk Treatment Program and governance (owners, timelines, risk acceptance).

2) Implement MDM/UEM for mobile/BYOD; conditional access and app protection for corporate email.

3) Deploy wireless security or prohibit Wi‑Fi with monitoring; document in policy.

4) Enforce data retention and destruction across live systems and backups; certify asset returns.

5) Remediate password storage practice—mandate prohibition of unencrypted records; scan/purge secrets.

6) Implement SoD for key management and adopt managed KMS/HSM with dual control.

7) Expand SDLC with SCA and SBOM; gate builds on critical dependency vulns.

8) Enhance API access management for clients (OAuth2 scopes, key lifecycle, rate limits).

9) Improve logging on network devices; centralize to SIEM; validate coverage.

This assessment is based on the provided questionnaire, policies, and SOC 2 reports. Residual risk remains High until the high-severity gaps are remediated and validated.