# ChatGPT Response

Below is Beaconer’s third-party risk summary for the vendor based on the provided documents (Security Questionnaire responses, Information Security Policy, Password Guideline, Azure and Logicworks SOC 2 Type 2, Network Diagram, and Privacy materials).

Rating Summary

• Inherent Risk: High

• Justification: Vendor processes/hosts PI/SPI and supports DSARs/GDPR (Questionnaire: Yes to PI/SPI processing, encryption at rest/in transit, DSARs, right to be forgotten). Cloud-hosted on Microsoft Azure and supported by Logicworks—both SOC 2 Type 2. Multiple integrations (e.g., Bullhorn, HubSpot, Gmail, LinkedIn) and use of subservice providers. Material business impact if compromised.

• Control Effectiveness: Partially Effective (≈60%)

• Justification: Strong infrastructure controls covered by Azure and Logicworks SOC 2s; however, significant control gaps exist in the vendor’s own program (no CISO; weak risk treatment governance; gaps in network hardening, wireless security, MDM, application security, vendor-risk inventory, and some crypto/key management practices).

• Residual Risk: High

• Reasoning (Matrix): High Inherent + Partially Effective → High

Control Testing Metrics

• % Control Coverage: ~60%

• Basis: Extensive “Yes” answers across many domains; Azure/Logicworks controls are audited (SOC 2); however, many “No” responses in the vendor questionnaire materially reduce coverage across Access, Network Security, AppSec, Mobile/MDM, DR, and Vendor Mgmt.

• Total Gaps Identified: 18

• Total Critical Gaps (High Severity): 10

• Residual Risk Calculation Explanation: Given the vendor handles PI/SPI with multi-cloud integrations and relies on subservice providers, inherent risk is high. While Azure/Logicworks SOC 2s evidence strong infra/security practices, the vendor’s control gaps (risk governance, CISO, network hardening/logging, wireless, MDM, key mgmt segregation, app security pipeline, DR testing) reduce overall effectiveness to “Partially Effective,” resulting in High residual risk per Beaconer matrix.

Section 3: Control Testing (Access Control Domain)

Control Question Vendor Response Evidence / Notes

Program approved & communicated Yes Questionnaire Q39; Information Security Policy in place

Regular access review for all Yes Q41/Q42: periodic access reviews and privileged reviews

IDs are auto terminated on last day Yes Q53: terminated IDs disabled on last day

Segregation of duties Yes Q52: SOD for granting/approving access

Controls for Corporate Email on personal phones No Q65 Yes but MDM controls are “No” (Q284-286) → control is insufficient; treat as No

MFA deployed Yes Q44/Q45: MFA deployed incl. privileged access

Application supports customer SSO Yes Q47: supports SAML/OpenID/SSO

Unique IDs required Yes Q48

Principle of least privilege Yes Q50

Password policy Yes Password Guideline (≥14 chars, rotation: 6 months user, quarterly system)

Process to request approval for Access Yes Q49

Password sharing prohibited Yes Q56

Passwords are salted & hashed at storage Yes Q63

Section 4: Gap Analysis

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

Risk Governance No formal risk treatment program (Q6); No designated CISO (Q13) High Lack of accountable ownership; unmanaged risks Establish ERM-aligned risk treatment program; appoint a CISO with charter and authority

Access Control No enforced session logoff policy (Q54); Acceptance of unencrypted password record not prohibited (Q61) Medium Credential persistence; local disclosure risk Enforce idle session lockouts; explicitly prohibit any plaintext password storage

Asset Mgmt No process to verify return of assets on termination (Q71) Medium Data leakage via unreturned assets Implement asset return checklist with HR/IT clearance gates

Vendor Risk Mgmt No remediation reporting for subcontractor issues (Q84); No third-party inventory (Q87) High Blind spots in supply-chain risks Implement third-party inventory & tiering; log/remediate supplier findings; require attestations (SOC2/ISO)

Network Security No hardening standards for network devices (Q166); Insufficient network device log detail (Q169); Wireless controls not implemented (Q176) High Unauthorized access, undetected lateral movement Publish and enforce hardened baselines (CIS); enable detailed device logging; implement WPA2/3-Enterprise and NAC; periodic config reviews

Mobile/MDM No BYOD MDM (Q284), no technical enforcement for PIN/encryption/remote wipe (Q285) High Loss/theft → data compromise Deploy MDM/UEM for all mobile endpoints; enforce device encryption, screen lock, remote wipe

DR/BCP Production data centers not included in DR tests (Q147) Medium Unproven resilience Include production-like failover scenarios; document RTO/RPO results

Cryptography/Key Mgmt No SoD for key mgmt vs. ops (Q237) High Key misuse risk Segregate HSM/KMS admin from ops; enforce dual control; log/audit key ops

Data Lifecycle No data retention/destruction process covering subcontractors (Q244) Medium Data over-retention with vendors Add subcontractor obligations for retention/destruction; audit adherence

Application Security No pre-prod security review testing (Q207); No SCA (Q213); Clients cannot manage API access (Q196) High Injection/Supply-chain vulnerabilities; excessive API exposure Institute SDL gates: SAST/DAST/SCA; threat modeling; API gateway with RBAC & customer-managed keys/tokens; secure-by-default configs

Containers Clients cannot restrict container usage on sensitive systems (Q292) Medium Container sprawl risk Define container policy; label sensitive workloads; enforce admission controls/OPA policies

Wireless Security Wireless network controls “No” (Q176) High Rogue/WEP/WPA risks Enforce enterprise Wi-Fi (802.1X), segmentation, WIPS/WIDS

Privacy Gaps mostly addressed; ensure subcontractor DPIAs and cross-border notices align with practices Medium Data transfer and processor duties Extend DPIA to subprocessors; ensure DPA/SSC terms with all vendors; map data flows

Training Security awareness present; ensure secure SDLC training for devs Low Developer mistakes Provide annual secure coding/AppSec training with OWASP Top 10

Physical Security Delegated to subservice (Azure/Logicworks SOC 2) Low Facility risks covered Continue annual SOC report reviews, track exceptions

Notes and Evidence Highlights

• Strong Infra Posture: Microsoft Azure (SOC 2 Type 2; multiple regions; encryption in transit TLS 1.2+, at-rest AES-256; key mgmt, SIEM/logging; DR/BCP) and Logicworks (SOC 2 Type 2; Security/Availability/Confidentiality; vulnerability mgmt; IDS; backup/replication; BCM/DR).

• Vendor Policies: Information Security Policy exists; Password Guideline requires ≥14 characters; rotation: 6 months user / quarterly system; encourages passphrases and MFA.

• Major Gaps from Questionnaire: Absent CISO; no formal risk treatment; several “No” answers in Network Security (hardening/wireless/logging), MDM/UEM, AppSec (SCA, pre-prod security testing), DR scope, vendor risk inventory and subcontractor remediation tracking, key mgmt SoD, data retention/destruction coverage for subcontractors.

Recommended Remediation Plan (Priority)

1) Governance: Appoint CISO; formalize risk treatment program and third-party risk inventory; quarterly risk committee.

2) Endpoint/MDM: Roll out MDM/UEM across all mobile endpoints; enforce encryption, PIN, remote wipe; restrict corporate email to managed devices.

3) Network/Wireless: Implement device hardening baselines (CIS), detailed device logging, and WPA2/3-Enterprise with NAC; periodic audits.

4) AppSec Pipeline: Mandate SDL gates (SAST/DAST/SCA), pre-prod security reviews, API gateway RBAC/SSO, and customer-managed API controls.

5) Crypto/Key Mgmt: Enforce SoD and dual-control for KMS/HSM with auditable logs.

6) DR/BCP: Expand DR testing to include production-like failover; track RTO/RPO.

7) Data Lifecycle & Vendors: Extend retention/destruction obligations to subcontractors; track remediation reporting for supplier issues.

This assessment reflects the current documentation and responses provided. Strengthening the identified gaps—especially governance, MDM, network hardening, and AppSec—should materially reduce residual risk from High to Medium.