# ChatGPT Response

Rating Summary

• Inherent Risk: High — Logicworks provides Managed Cloud Operations with administrative access to customer environments and data; relies on subservice organizations (AWS, Azure, Equinix); business critical uptime and security are in scope.

• Control Effectiveness: Mostly Effective (95%) — SOC 2 Type 2 (02/01/2022–01/31/2023) with an unqualified opinion and no exceptions. A few controls were not tested due to no triggering events (e.g., no media disposals, no incidents). Dependencies on subservice organizations introduce residual exposure despite strong internal controls.

• Residual Risk: Medium — High inherent risk combined with Mostly Effective controls maps to Medium per Beaconer matrix.

Control Testing Metrics

• % Control Coverage: ~95% (broad SOC 2 coverage across CC, A1, C1 criteria; multiple supporting policies/procedures; continuous monitoring, vulnerability management, IR, BC/DR tested)

• Total Gaps Identified: 4

• Total Critical Gaps: 0

• Residual Risk Calculation Explanation: High Inherent + Mostly Effective (95%) = Medium per Residual Risk Matrix. No high-severity findings in Logicworks SOC 2; however, reliance on subservice orgs (Azure/AWS) includes known exceptions (Azure SOC 2) that add dependency risk.

Control Testing (Access Control)

Control Question Vendor Response Evidence / Notes

Program approved & communicated Yes Information security policies documented, version-controlled, reviewed, approved, and communicated (SOC 2 CC5.3, CC2.2)

Regular access review for all Yes Bi‑monthly access reviews performed; sampled reviews showed no changes required (SOC 2 CC6.2)

IDs are auto terminated on last day Yes Termination checklist; access revoked within 24 hours (SOC 2 CC6.2)

Segregation of duties Yes Prod migration restricted; developers require reviewed changes (SOC 2 CC6.3, CC8.1)

Controls for Corporate Email on personal phones No Not evidenced in SOC 2 or provided policies

MFA deployed Yes Remote production access requires MFA over encrypted VPN (SOC 2 CC6.1)

Application supports customer SSO No N/A to a single “app”; Logicworks uses Okta internally; customer SSO support not evidenced

Unique IDs required Yes Authentication requires unique usernames/passwords or authorized SSH keys (SOC 2 CC6.1)

Principle of least privilege Yes Access based on job role; privileged access restricted (SOC 2 CC6.3)

Password policy Yes 12+ chars, complexity, lockout, 90-day change (SOC 2 CC6.1)

Process to request approval for Access Yes Access request form + manager approval (SOC 2 CC6.2)

Password sharing prohibited No Not explicitly evidenced in SOC 2/policies provided

Passwords are salted & hashed at storage No Not explicitly evidenced; SOC 2 validates password configuration/controls but not storage hashing details

Gap Analysis

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

Access Control Lack of stated control for corporate email on personal devices Medium Data leakage via unmanaged endpoints Adopt and enforce MDM/MAM with conditional access; update policy and attestations

Access Control Customer SSO support not evidenced Low Potential friction, inconsistent auth posture for client integrations Confirm and document SSO options/integrations for client-facing portals/tools; publish in client runbook

Access Control Password sharing prohibition not explicitly stated Low Risk of credential sharing in edge cases Add explicit prohibition in AUP/InfoSec policy; reinforce via annual training

Cryptographic Controls Password storage hashing/salting not evidenced Medium Credential compromise blast radius Attest to hashing (e.g., bcrypt/scrypt/Argon2) with salts for any internally stored secrets; include in policy/architecture docs

Monitoring & IR Subservice: Azure break‑glass alerting had gaps (first half of period) per Azure SOC 2 Medium Delayed detection of emergency access in CSP estate Verify and document that Azure break‑glass alerting is enabled across all subscribed tenants; periodic control validation

Key Management Subservice: Azure secret rotation exceptions (2/26), network device password rotation exceptions (28/39) Medium Stale secrets increase exposure Obtain evidence of remediation and include in vendor monitoring; increase oversight cadence on subservice org control health

BCP/DR No issues noted in SOC2; plans tested Low — Continue annual tests; include subservice DR dependencies in tabletop exercises

Privacy No privacy program evidence in provided pack (privacy not in SOC 2 scope) Low Stakeholder expectations (DPIA, data rights flows) Request privacy policy and data subject rights handling documentation; align with customer data processing needs

Training No explicit note on secure email/mobile use training Low User behavior risks Augment security awareness with secure mobile/email modules; track completion

Physical Security Carved out to subservice orgs (Equinix/AWS/Azure) Low Dependency on colocation/cloud physical controls Continue annual review of subservice SOC reports and track exceptions

Notes and Evidence Cross‑References

• Logicworks SOC 2 Type 2 (02/01/2022–01/31/2023): Unqualified; controls operating effectively; several controls “not tested” due to no triggering events (e.g., media destruction, incidents) — not exceptions.

• Microsoft Azure SOC 2 Type 2 (04/01/2022–03/31/2023): Unqualified with noted exceptions:

• OA‑15: 28/39 network devices not rotated per cadence.

• OA‑20: Break‑glass alerting not enabled for 2 of 4 domains for part of the period; later remediated.

• DS‑1: 2/26 secrets not rotated per cadence.

• LA‑7: 2/19 offerings had mismatched quotas. Management indicated remediation.

• D3 Information Security Policy (policy-level): NIST‑aligned; passwords 90 days; MFA; VPN controls; backups; encryption TLS 1.2; supports Azure-based hosting. Policy confirms expectations but is not audited evidence.

• Organizational dependencies: Equinix colocation and AWS/Azure platforms (complementary subservice organization controls).

Residual Risk Narrative

Logicworks’ managed cloud controls are strong and operating effectively (SOC 2). The inherent risk is high due to the nature of services (privileged access, multi-tenant cloud dependencies). Subservice organizations (Azure/AWS/Equinix) are appropriately monitored; however, Azure SOC 2 noted several non-critical exceptions (secret rotation, break‑glass alerting for a portion of the period, network device password rotation), which slightly reduce overall control assurance across the full stack. With Mostly Effective controls (95%) and subservice monitoring, residual risk is Medium per Beaconer matrix.

Recommended Follow‑Ups (Vendor Management)

• Obtain and review Azure/AWS current SOC 2 reports each cycle; specifically verify remediation status of prior Azure exceptions and any new exceptions.

• Request explicit attestations from Logicworks on password storage hashing/salting for any local identity stores (or confirm exclusive use of Okta/IdP).

• Confirm and document corporate mobile/email security controls (MDM/MAM) and update training content and policy references.

• Validate that break‑glass alerting is enabled and periodically tested across all managed Azure/AWS tenants.

• Ensure privacy documentation (policy, DSR handling, DPIA approach) is provided if processing personal data under the engagement.