TRULY AGENTIC (INDEPENDENT ENGINEERING PRACTICE — ANIL PERVAIZ)

CSA CAIQ-Lite (BYOC) v4.0

Cloud Security Alliance CAIQ-Lite self-assessment tailored to Truly Agentic Bring-Your-Own-Cloud (BYOC) architecture, zero data egress, customer KMS custody, and fail-closed audit logging.

November 24, 2026

Security Questionnaire Response

https://trulyagentic.io

security@trulyagentic.io

Response Summary

Answer	Count	Percentage
Yes	12	85.7%
Partial	1	7.1%
No	0	0.0%
N/A	1	7.1%
Total	14	100%

BYOC Architecture & Data Isolation

3/3 controls satisfied

ID	Question	Answer	Explanation
AIS-01	Where is customer operational data processed and stored?	YES	Operational payloads (ERP rows, invoices, CRM exports, OAuth refresh tokens, and audit ledgers) remain exclusively inside the customer-owned AWS, GCP, or Azure VPC/VNet. Truly Agentic operates zero multi-tenant SaaS holding client business data.
AIS-02	Are customer prompts, operational records, or telemetry used to train foundation models?	YES	No. Deployments connect exclusively to customer-controlled private VPC endpoints (AWS Bedrock PrivateLink, GCP Vertex AI Private Service Connect, or Azure OpenAI Private Endpoint) or contractual zero-data-retention configurations with model training disabled.
AIS-03	Is network access to the runtime isolated from public ingress?	YES	Terraform starters deploy runtimes into private VPC subnets with no public inbound exposure. Local BYOC containers bind strictly to 127.0.0.1 for private tunnel/VPC routing.

Encryption & Key Custody

2/2 controls satisfied

ID	Question	Answer	Explanation
CEK-01	Who retains cryptographic root key custody and secret lifecycle control?	YES	Customers retain root custody via AWS KMS/Secrets Manager, GCP Cloud KMS/Secret Manager, or Azure Key Vault. Agent runtimes receive only scoped short-lived credentials tied to OIDC workload identity.
CEK-02	Is data encrypted in transit and at rest with modern algorithms?	YES	Public web edges enforce HTTPS with TLS 1.2+ on Cloudflare; customer BYOC buckets, ledgers, and secrets vaults use customer-managed KMS encryption with automated key rotation enabled.

Identity, Access & Approval Controls

3/4 controls satisfied

ID	Question	Answer	Explanation
IAM-01	Are AI agents prevented from sharing personal or root administrator credentials?	YES	Control 1 (AgentRegistry / isValidServiceAccount) validates scoped workload service accounts (svc-agent-*) in code and rejects personal email addresses, root accounts, and shared admin handles.
IAM-02	Are irreversible write actions separated from read and draft workflows?	YES	Control 2 (PolicyEngine) isolates read, propose, and write tiers across Five Levels of Agency (L1–L5), while Control 3 (ApprovalGate + Slack HMAC) requires sign-off from a named individual human approver (usr_*).
IAM-03	Does Truly Agentic retain standing access to customer cloud accounts post-handover?	YES	No. Weeks 1–2 run strictly read-only on replicas/snapshots; Weeks 3–4 run shadow mode without mutating ERPs; temporary onboarding SSO/VPN leases auto-expire upon handover.
IAM-04	Does Truly Agentic store multi-tenant SaaS end-user passwords?	NA	Not applicable. There is no multi-tenant SaaS control plane or hosted customer password database; authentication delegates to each customer IdP via OIDC/SAML or workload identity.

Audit Logging & Fail-Closed Guarantees

2/3 controls satisfied

ID	Question	Answer	Explanation
LOG-01	What happens when the audit logging sink is unreachable or errors?	YES	Control 5 enforces "No Log, No Action": GovernanceGateway commits a SHA-256 hash-chained pre_execution row before calling any downstream tool. Ledger errors abort execution cleanly with zero external mutations.
LOG-02	Are audit records protected against retrospective tampering?	YES	PostgreSQL trigger trg_audit_ledger_immutable raises an exception on UPDATE or DELETE, hash links validate via verifyAuditChainEntries, and Terraform starters configure S3 Object Lock / GCS Retention Lock WORM buckets.
LOG-03	Is there an independent third-party SOC 2 Type II or ISO 27001 audit report?	PARTIAL	Controls are engineered and mapped to SOC 2 TSC and ISO 27001:2022 Annex A ahead of formal audit, but Truly Agentic is currently Pre-SOC 2 (no third-party CPA attestation yet). Complete source/IaC review is available under Mutual NDA.

Supply Chain, Disclosure & Authorized Testing

2/2 controls satisfied

ID	Question	Answer	Explanation
IVS-01	How is build pipeline and MCP tool supply-chain integrity protected?	YES	Public governance kit CI pins GitHub Actions by commit SHA with minimal permissions, enforces TypeScript strict checks, and validates MCP tool schemas against pinned SHA-256 manifest digests.
TVM-01	How are vulnerability reports and active security tests authorized?	YES	Coordinated disclosure is published at https://trulyagentic.io/.well-known/security.txt (security@trulyagentic.io). Active security tests run only on synthetic harnesses or customer sandboxes after executing written Schedule B authorization.