ARCANA RESEARCH

CAIQ Lite Questionnaire

Cloud Security Alliance Consensus Assessments Initiative Questionnaire (v4 short form). Pre-filled responses for vendor security review. Effective April 24, 2026.

How to use this document. Marcus from your TPRM team can ingest this directly into your vendor risk tool, or use the answers below as the basis of a SIG Lite response. Notes below each answer point to the evidence (config, contract clause, or page on arcana-research.com). For inherited controls from our subprocessors, request the underlying SOC 2 reports via compliance@arcana-research.com.

AAC AUDIT ASSURANCE & COMPLIANCE

AAC-01 Do you produce audit assertions using a structured industry framework (e.g., SOC 2, ISO 27001)?

Partial. SOC 2 Type 1 readiness in progress; Type 2 audit window 2026. Inherited SOC 2 Type 2 from all hosting subprocessors.

AAC-02 Are independent third-party audits performed at least annually?

No. First external pen test scheduled 2026. SOC 2 audit scheduled 2026.

AAC-03 Do you make audit reports available to tenants on request?

Yes. Inherited subprocessor SOC 2 reports available under NDA. Our own SOC 2 will be available once issued.

BCR BUSINESS CONTINUITY & OPERATIONAL RESILIENCE

BCR-01 Do you have a documented business continuity / disaster recovery plan?

Partial. Hosting and database providers (Vercel, Turso) provide automated backups and multi-region failover. Application-level DR runbook in development.

BCR-02 Are backups encrypted at rest?

Yes. AES-256, provider-managed keys.

BCR-03 What is the documented RTO / RPO?

Partial. Targeted RTO: 4 hours. Targeted RPO: 24 hours. Formal SLA available with paid programs.

CCC CHANGE CONTROL & CONFIGURATION MANAGEMENT

CCC-01 Are production changes peer-reviewed before deployment?

Yes. All production deploys go through pull request review and pass automated checks (CI lint, type, build).

CCC-02 Is unauthorized software prevented from running in production?

Yes. Production deploys are pinned to specific Vercel deployments; only signed-off code from main branch reaches production.

DSI DATA SECURITY & INFORMATION LIFECYCLE

DSI-01 Is sensitive data classified and inventoried?

Yes. Data scope documented at /security and /privacy. No PHI, payment, or consumer data.

DSI-02 Is data encrypted in transit?

Yes. TLS 1.2+ enforced; HSTS enabled.

DSI-03 Is data encrypted at rest?

Yes. AES-256 via provider-managed keys (Turso, Supabase, Vercel).

DSI-04 Are secure data deletion procedures in place?

Yes. Self-serve account deletion; processed within 30 days. Subprocessor deletion follows their respective SLAs.

DSI-05 Is customer data segregated from other tenants?

Yes. Per-respondent rows in shared tables, scoped by user_id and workspace_id; row-level access enforced in application layer.

DSI-06 Are tenants notified before subprocessor changes?

Yes. 14 days notice via email to active members; subprocessor list maintained at /security.

EKM ENCRYPTION & KEY MANAGEMENT

EKM-01 Are cryptographic keys managed by a provider-grade KMS?

Yes. Provider-managed keys at Vercel, Turso, Supabase. No customer-held keys.

EKM-02 Are passwords stored using a one-way hash with salt?

Yes. bcrypt with cost factor 10.

EKM-03 Are secrets and API keys rotated regularly?

Partial. Rotated on staff offboarding and on suspicion of compromise. No fixed rotation calendar.

GRM GOVERNANCE & RISK MANAGEMENT

GRM-01 Do you have documented information security policies?

Partial. Privacy Policy, Terms of Service, DPA, and Security Overview published. Internal information security policy formalization in progress as part of SOC 2 readiness.

GRM-02 Are risk assessments performed periodically?

Partial. Vendor risk assessments performed prior to onboarding any new subprocessor. Formal periodic enterprise risk assessment scheduled as part of SOC 2 cadence.

GRM-03 Is there an information security officer or equivalent role?

Yes. Security and incident response responsibilities held by founder; reachable at security@arcana-research.com.

HRS HUMAN RESOURCES

HRS-01 Are background checks performed on personnel with access to customer data?

Partial. Performed for full-time employees and contractors with production access.

HRS-02 Are personnel required to acknowledge confidentiality and security policies?

Yes. All personnel sign confidentiality agreements; founders bound by company operating agreement.

IAM IDENTITY & ACCESS MANAGEMENT

IAM-01 Is multi-factor authentication required for administrative access?

Yes. Enforced on all production console access (Vercel, Turso, Supabase admin, GitHub).

IAM-02 Is access provisioned on a least-privilege basis?

Yes. Role-based access. Production database direct access restricted to founder.

IAM-03 Is access revoked promptly on role change or termination?

Yes. Standard offboarding checklist; access to all production systems removed within 24 hours.

IAM-04 Is SSO/SAML supported for enterprise customers?

Partial. SSO/SAML available on request as part of paid enterprise programs.

IAM-05 Are user passwords subject to a documented password policy?

Yes. Minimum 8 characters; rejects ~65 common and previously-breached passwords; rejects email-equivalent passwords.

IAM-06 Are failed authentication attempts rate-limited?

Yes. Per-IP: 20 attempts / 15 min on login (10 / hr on register). Per-email: 5 attempts / 15 min — blocks credential-stuffing across rotating IPs.

IVS INFRASTRUCTURE & VIRTUALIZATION SECURITY

IVS-01 Are network communications encrypted in transit?

Yes. TLS 1.2+ end-to-end; HSTS enabled.

IVS-02 Is application logging enabled and retained?

Yes. Application and access logs retained 90 days minimum at Vercel.

IVS-03 Are systems scanned for vulnerabilities?

Yes. Automated dependency scanning on every push; high-severity advisories patched within 7 days. Static analysis and secret scanning in CI.

SEF SECURITY INCIDENT MANAGEMENT, E-DISCOVERY & CLOUD FORENSICS

SEF-01 Do you have a documented incident response process?

Yes. Internal IR runbook covering detection, containment, eradication, recovery, and notification.

SEF-02 Are tenants notified of confirmed security incidents within a defined timeframe?

Yes. Notification without undue delay, in any case within 72 hours of confirmation, in alignment with GDPR Article 33 and US state-law timelines.

SEF-03 Is there a process for responsible vulnerability disclosure?

Yes. Disclosure to security@arcana-research.com. Good-faith research encouraged; no legal action for testing within standard responsible-disclosure norms.

STA SUPPLY CHAIN MANAGEMENT, TRANSPARENCY & ACCOUNTABILITY

STA-01 Is a list of subprocessors made publicly available?

Yes. Published at /security and /security/brief. Updated with at least 14 days notice before adding any subprocessor.

STA-02 Are subprocessors bound by data-protection obligations equivalent to your own?

Yes. DPAs in place with all material subprocessors; LLM subprocessors include zero-retention contractual terms.

TVM THREAT & VULNERABILITY MANAGEMENT

TVM-01 Are penetration tests performed by independent third parties?

No. First independent pen test scheduled 2026.

TVM-02 Is a malware-protection program in place?

Yes. No execution of customer-supplied code in production. CSP and sandbox controls inherited from Vercel.

For questions, follow-ups, or to request the most recent version of this document with amendments since the issue date, email compliance@arcana-research.com. SIG Lite version available on request from named-account procurement teams.